2010-03

Establishment of the National Maritime Intelligence Center : understanding the foundations of trust to support a collaborative environment in homeland security

Caswell, Kenneth L.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ESTABLISHMENT OF THE NATIONAL MARITIME INTELLIGENCE CENTER: UNDERSTANDING THE FOUNDATIONS OF TRUST TO SUPPORT A COLLABORATIVE ENVIRONMENT IN HOMELAND SECURITY

by

Kenneth L. Caswell Jr.

March 2010

Thesis Advisor:	Erik Dahl
Second Reader:	Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Establishment of the National Maritime Intelligence Center: Understanding the Foundations of Trust to Support a Collaborative Environment in Homeland Security			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kenneth L. Caswell Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited**.**			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

On January 14, 2009, the former Director of National Intelligence (DNI), Admiral Mike McConnell (ret.), established The National Maritime Intelligence Center (NMIC). The NMIC was created to serve as the national focal point for maritime intelligence, ensuring a unified national effort to execute the Maritime Strategy and the National Strategy for Maritime Security (NSMS) at all levels of government. The establishment of the NMIC is part of the Navy's response to an Intelligence Community Directive through which the DNI challenged all intelligence community (IC) elements to establish an "analytic outreach" initiative to "engage with individuals outside the intelligence community to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information." That directive had been a response to recommendations from the 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report, which recommended that, "IC analysts broaden their information horizons by collaborating with... expertise wherever it resides…" This thesis will examine the question: Can the NMIC design and create a culture of trust and collaboration that collectively draws input from analyst, collector, and customer to effectively support maritime domain awareness intelligence support regarding homeland security?

14. SUBJECT TERMS Trust, Collaborative Environment, Inter-Agency, Maritime Intelligence			**15. NUMBER OF PAGES** 83
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ESTABLISHMENT OF THE NATIONAL MARITIME INTELLIGENCE CENTER; UNDERSTANDING THE FOUNDATIONS OF TRUST TO SUPPORT A COLLABORATIVE ENVIRONMENT IN HOMELAND SECURITY

Kenneth L. Caswell Jr.
Lieutenant, United States Navy
B.A. Hawaii Pacific University 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2010**

Author: Kenneth L. Caswell Jr.

Approved by: Erik Dahl
Thesis Advisor

Captain Robert Simeral, USN (Ret.)
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

On January 14, 2009, the former Director of National Intelligence (DNI), Admiral Mike McConnell (ret.), established The National Maritime Intelligence Center (NMIC). The NMIC was created to serve as the national focal point for maritime intelligence, ensuring a unified national effort to execute the Maritime Strategy and the National Strategy for Maritime Security (NSMS) at all levels of government. The establishment of the NMIC is part of the Navy's response to an Intelligence Community Directive through which the DNI challenged all intelligence community (IC) elements to establish an "analytic outreach" initiative to "engage with individuals outside the intelligence community to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information." That directive had been a response to recommendations from the 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report, which recommended that "IC analysts broaden their information horizons by collaborating with... expertise wherever it resides…" This thesis will examine the question: can the NMIC design and create a culture of trust and collaboration that collectively draws input from analyst, collector, and customer to effectively support maritime domain awareness intelligence support regarding homeland security?

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABD	Air Bridge Denial Program
CIA	Central Intelligence Agency
CONOPS	Concept of Operations
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
GMII	Global Maritime Intelligence Integration
IC	Intelligence Community
ICC	Coast Guard Intelligence Coordination Center
ISE	Information Sharing Environment
JIATF-S	Joint Inter-Agency Task Force South
ONI	Office of Naval Intelligence
LASD	Los Angeles Sheriff's Department
LET	Lashker-e-Taiba
MDA	Maritime Domain Awareness
MOTR	Maritime Operational Threat Response
NCTC	National Counter Terrorism Center
NGA	National Geo-Spatial Agency
NMIC	National Maritime Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSMS	National Strategy for Maritime Security
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The completion of this project would not have been possible without the love and support of my wife, Lacey, and my great kids, Madeline, Kenny, and Jackson. Thank you for your love and imagination and for never letting me give up; you all truly inspire me. To my thesis advisor, Erik Dahl, and second reader, Robert Simeral, I would like to thank two great Americans who have dedicated their lives to serving our great nation. Your support and direction made this all possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. ESTABLISHMENT OF THE NATIONAL MARITIME INTELLIGENCE CENTER

On January 14, 2009, the former Director of National Intelligence (DNI), Admiral Mike McConnell (ret.), established The National Maritime Intelligence Center (NMIC). The NMIC was created to serve as the national focal point for maritime intelligence, ensuring a unified national effort to execute the Maritime Strategy and the National Strategy for Maritime Security (NSMS) at all levels of government.[1] The establishment of the NMIC is part of the Navy's response to an Intelligence Community Directive[2] through which the DNI challenged all intelligence community (IC) elements to establish an "analytic outreach" initiative to "engage with individuals outside the intelligence community to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information."[3] That directive had been a response to recommendations from the 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report, which recommended that "IC analysts broaden their information horizons by collaborating with... expertise wherever it resides…"[4]

B. RESEARCH QUESTION AND METHODOLOGY

This thesis will examine the questions: Can the NMIC design and create a culture of trust and collaboration that collectively draws input from analyst, collector, and customer to effectively support maritime domain awareness intelligence support regarding homeland security? Can it meet the challenge posed by the Director of National Intelligence and the WMD Commission?

---

1 Regina McNamara CDR USCG, "Ribbon Cutting Establishes the New National Maritime Intelligence Center," http://www.navintpro.org/associations/4202/files/quarterly/NIPQIndex.htm (accessed 6/9/2009).

2 Office of The Director of National Intelligence, Intelligence Community Directive 205: Analytic Outreach.

3 Ibid.

4 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, http://govinfo.library.unt.edu/wmd/report/index.html (accessed 5/15/2009).

A culture-of-collaboration approach is about "maximizing time, talent and tools to create value based on [the] collective efforts" of contributors, participants and consumers of intelligence.[5] In collaborating across federal, state, and local cultures, there is a dynamic that produces a broader perspective and creates greater value in the final product and has equal value amongst all participants. This is particularly true when it comes to solving complex analytic problems that affect multiple customers in different ways. This concept has three distinct characteristics that differ from the traditional isolated and stove-piped method of intelligence production: it acts as a force multiplier in an emerging threat environment that folds in new homeland security customers with a different perspective; it develops a community of interest that fosters information sharing and communication to effectively address time-sensitive threat warnings within the maritime domain; and lastly, it supports the call to create a culture of collaboration and revive imagination within the IC by challenging assessments and offering alternative analyses from a shared working group. This newly established NMIC, in its early development, has the opportunity to review cases of successful collaboration in order to establish and develop a trusted culture-of-collaboration network to answer the mandate for intelligence reform from a need-to-know institution to a responsibility-to-provide network.[6]

This thesis will argue that a culture of collaboration structured around the theoretical principles of trust building will prove successful in drawing input from the Maritime Community of Interest to effectively support a unified response to maritime domain awareness efforts with regard to homeland security. Similar to the design and complement of the Joint Interagency Task Force-South (JIATF-S) command design, which requires a unified response from various agencies and nations to combat drug trafficking, the NMIC will require a similar trusted environment to cover the complexity of challenges within the maritime domain. This thesis will address the need for collaboration amongst a wide array of agencies and institutions with maritime responsibility to effectively provide a unified response to maritime security.

---

5 Evan Rosen, The Culture of Collaboration, 1st ed., http://www.thecultureofcollaboration.com/ (accessed 5/21/2009).

6 Office of the Director of National Intelligence, United States Intelligence Community: Information Sharing Strategy.·

As stated in the National Strategy for Maritime Security: "The maritime domain in particular presents not only a medium by which threats can move, but offers a broad array of potential targets that fit the terrorists' operational objectives of achieving mass casualties and inflicting catastrophic economic harm."[7] It should be viewed as a priority and a necessity to identify avenues of collaboration between stakeholders at all levels of government to protect our maritime interests as effectively as possible. This proposed intelligence culture shift from stove-piped intelligence agencies, that incorporates elements of local, state, and federal entities with a vested interest in maritime security, could act as a nexus for future collaboration efforts concerning critical intelligence issues.

C. LITERATURE REVIEW

1. The Call for Intelligence Reform

No aspect of the U.S. government has received more attention since 9/11 than intelligence reform, and rightfully so. As former 9/11 Commission Vice Chairman Lee Hamilton stated, "The single most important tool that we have in preventing terrorist attacks is intelligence."[8] So why has intelligence reform been such a slow process? The problem lies within structure, culture, and identifying the proper balance between security and disseminating information to trusted sources. Amy Zegart points out that there is a significant difference between change and adaptation, "The key issue is whether those changes matter, or more precisely, whether the rate of change within an organization keeps pace the rate of change in the external environment."[9] For the most part, the current structure of the intelligence community and intelligence cycle is one that has stood strong since the end of WWII.[10]

The predominant threat and focus of effort for the IC from the end of WWII through the early 1990s was the Soviet Union. The intelligence structure formed around

---

7 United States Department of Homeland Security, The National Strategy for Maritime Security.·

8 Lee Hamilton, "Hamilton Shares Thoughts on 9/11." http://www.homepages.indiana.edu/102204/text/hamilton.shtml (accessed 5/15/2009).

9 Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, New Jersey: Princeton University Press, 2007), 20.

10 Robert M. Clark, Intelligence Analysis: A Target Centric Approach.

this adversarial giant, whose large footprint, over decades, created predictable patterns to use for indications and warnings. After the fall of the Soviet Union, the re-shaping of the intelligence structure was frequently recommended, but intelligence organizations and officials, rooted in a traditional IC culture, fought the need, and the call for, a drastic overhaul.[11] In today's world, the United States faces a determined and innovative adversary who is willing to exploit the maritime domain to further their cause. As U.S. Coast Guard Commandant Admiral Thad Allen points out, "…the threats we face in the maritime commons [today] tend to be agnostic to political boundaries and traditional jurisdictions."[12] Whether it is drug cartels smuggling narcotics in semi-submersibles, locally born extremist movements with a grudge against the government, or a global jihadist movement looking to find security vulnerabilities within a major port facility, the threat is real and emerging. Gregory Treverton of RAND notes that, "To truly reshape intelligence gathering in order to meet today's threats, all of the Cold War Legacy must be put on the table…"[13]

Intelligence reform and organizational change is not actually a new concept, at least not in the way of review by official commissions, studies and recommendations to improve the coordination processes. As Amy Zegart points out:

> Between the fall of the Soviet Union in 1991 and September 11, 2001, no fewer than twelve major bipartisan commissions, governmental studies, and think tank task forces examined the U.S. Intelligence Community… All twelve reports offered not only extensive discussion of key problems but specific recommendations to fix them.[14]

Intelligence reform is not only a call for re-structuring intelligence, but about a change in the culture of intelligence and understanding the underpinnings that allow trusted environments of collaboration to prosper. The Intelligence Reform act of 2004

---

11 Zegart, *Spying Blind,* 31.

12 Otto Kreisher, "Collaborative Approach, U.S. Maritime Operational Threat Response Plan Coordinates Federal Action in Ports and Far from Shore." *Seapower* (5/2009).

13 Gregory Treverton, "Intelligence Test: Post 9/11 Intel Reform Has Been in Name Only. To Make America Safer, We Need Fundamental Change Across the Entire Government." *Democracy: A Journal of Ideas,* Winter 2009, no. 11, http://www.democracyjournal.org/article.php?ID=6667 (accessed 5/15/2009).

14 Zegart, *Spying Blind,* 27–28.

offers the foundation for moving in the right direction regarding intelligence reform.[15] The Act created the Office of the Director of National Intelligence, charged with "establish[ing] objectives and priorities for the intelligence community" and managing the overall process of national intelligence.[16] The Act also granted the DNI the authority to create a National Counter Terrorism Center to integrate foreign and domestic counterterrorism intelligence collection and analysis and strategic planning in support of operations.[17] In addition to creating the position of DNI, the Intel Reform Act also answered the president's directive for establishing an Information Sharing Environment (ISE) that would "facilitate the sharing of terrorism information among all appropriate federal, state, local, tribal and private sector entities, through the use of policy guidelines and technologies." The ISE's scope was later expanded as a result of the Implementing Recommendations of the 9/11 Commission Act of 2007 to include homeland security information and weapons of mass destruction information as well.[18] The Intelligence Reform Acts provisions were primarily designed to foster coordination and encourage culture change across the intelligence community, which is a complete culture shift from the traditional design of the IC. These initiatives require buy-in across the IC in order to effectively establish the needed collaborative environment necessary, with members of the interagency, to address the threats of the twenty-first century.

The doctrine to direct reform within the intelligence community has been clearly written, but merely changing the organizational charts within national intelligence does not answer the call for reform.[19] The true test of reform will be found by identifying why cultural barriers exist and what causes the derailment of information sharing. In addition, identifying exactly who the customers are, understanding their needs is a critical step toward creating a culture of collaboration.

---

15 Gregory Treverton and Peter Wilson, "True Intelligence Reform is Cultural, Not Just Organizational Chart Shift," *The Christian Science Monitor* www.rand.org/commentary/2005/01/13/CSM.html (accessed 5/15/2009).

16 United States Senate Committee on Governmental Affairs, Summary of Intelligence Reform and Terrorism Prevention Act of 2004, hsgac.senate.gov/public/_files/ConferenceReportSummary.doc (accessed 5/15/2009).

17 Ibid.

18 United States Government, National Strategy for Information Sharing.

19 Treverton and Wilson, True Intelligence Reform is Cultural, Not Just Organizational Chart Shift."

2. Maritime Domain Awareness—Identifying Seams in the System

The United States government has identified three primary responsibilities in regards to maritime security:

1. Produce and distribute timely and accurate threat advisory and alert information as well as appropriate protective measures to state, local, and tribal governments and the private sector, via a dedicated homeland security information network;

2. Provide guidance and standards for reducing vulnerabilities

3. Provide an active, layered, and scalable security presence to protect from and deter attacks.[20]

The Department of Homeland Security has identified and broadly categorized the potential actors threatening the maritime domain to include nation-states, terrorists, and transnational criminals and pirates.[21] These three categories help to better define the potential threats the NMIC faces, while also addressing the complexity of the issue of responding to all of them. The idea of creating threat scenarios and identifying potential avenues of attack is not a new concept for the United States. In fact, well before the Japanese attack on Pearl Harbor, U.S. Navy planners developed a threat scenario around a carrier-based air attack. Unfortunately, Navy leadership in Washington and Hawaii did not consider the scenario a realistic one.[22] The process more commonly referred to today as "red-teaming" was recommended in the 9/11 Commission Report, the Senate Intelligence Committee Report on Iraq's WMD programs, and the Butler Report.[23] All three reports faulted groupthink of intelligence failures and called on alternative analyses

---

20 United States Department of Homeland Security, The National Strategy for Maritime Security.

21 Ibid.

22 Gordon Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: McGraw-Hill, 1981), 41.

23 National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, 567, http://isbndb.com/d/book/the_9/11_commission_report_final_report_of_the_national_comm (accessed 5/20/2009). United States Congress, Senate Intelligence Committee on Intelligence — Postwar Findings on Iraq's WMD Programs and Links to Terrorism and how they Compare with Prewar Assessments, http://intelligence.senate.gov/phaseiiaccuracy.pdf (accessed 6/6/2009). United Kingdom House of Commons, The Butler Report — Review of Intelligence on Weapons of Mass Destruction, http://www.archive2.official-documents.co.uk/document/deps/hc/hc898/898.pdf (accessed 6/6/2009).

and the need to exercise imagination as a routine matter.[24] To effectively address the myriad of threats the maritime domain faces, it is essential to have: "integrated all-source intelligence, law enforcement information, and open-source data from the public and private sectors."[25]

Local law enforcement patrolling the shores of the United States received a wake-up call for collaboration after witnessing the Mumbai attack's success in November 2008. Less than a dozen operatives were able to shut down a city the size of Los Angeles by creating organized chaos throughout the streets of Mumbai.[26] Those responsible for responding to and preventing similar attacks are well aware of the trends and are adjusting accordingly. In April 2009, The Los Angeles Sheriff's Department (LASD) held a workshop to address "Mumbai-style" attacks within the Los Angeles region in order to address the concepts of incident command, unified command, multiple emerging simultaneous incidents, and unified action within the region.[27] This preliminary tabletop discussion included players from the Los Angeles Sheriff's Department, Los Angeles Police Department, Los Angeles County Fire Department, Mass Transit Authority, and the Federal Bureau of Investigation. This tabletop exercise created heated discussions over "who's in charge" in such a chaotic and multi-threat environment and how to coordinate and respond effectively with limited resources. Heated or not, it was viewed by one seasoned sergeant in the LASD as "probably in the top three of my career, for best participation at a command level."[28] These issues are tough to work through, mostly because of cultural barriers in organizations. However, the Los Angeles County first responders realize the catastrophic consequences likely if they do not collaborate. In May 2009, an actual live exercise was scheduled to take place to work out the

24 National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, 567).

25 United States Department of Homeland Security, The National Strategy for Maritime Security.

26 Rosa Brooks, "War on Terror —an Exercise in Folly," *Los Angeles Times*, sec. Opinion, 04 12/2008, http://www.latimes.com/news/opinion/la-oe-brooks4-2008dec04,0,6204083.column (accessed 6/1/2009).

27 James Sully, SGT, Personal e-mail concerning Command Workshop for Common Ground Exercise In LA County.

28 Sully, personal e-mail.

relationship between fusion center and responding authorities and to stress-test the relationship of Los Angeles County first responders. The results of this exercise have not been made available to the public at this time.

The tactics used in the Mumbai attack were proven to be effective in causing mass chaos for both civilians and responding authorities. There was an obvious disconnect, not only between first responders, but also between intelligence agencies and government authorities as well. Not only did U.S. officials warn India of an imminent sea-borne attack, they warned twice.[29] Local Indian officials who have reviewed the Mumbai attacks have pointed out that the only way to have stopped the Mumbai attacks would have been to respond while the Lashker-e-Taiba (LeT) operatives were still at sea. What role will the NMIC play in coordinating and releasing threat warnings to first responders that have responsibility for maritime security? Local authorities are already exercising the relationship and coordination piece so they can respond accordingly, but has the information pipeline been identified to relay threat warnings from national intelligence?

3. A Collaborative Intelligence Environment

There is no such thing as information sharing; there is only information trading.[30]

Academics, business leaders, and others have discussed and written about collaboration and team building for decades. There is a great deal of discussion in the collaboration literature examining the elements of success in a collaborative endeavor. Back in 1999, the MITRE Corporation conducted a survey of the IC documenting the factors inhibiting collaboration. MITRE concluded the following:

> … a strong competitive culture exists among the agencies. A key factor driving competition is the budget process in which agencies vie for resources. IC agencies more typically publish intelligence reports in competition with each other as opposed to collaborating on joint efforts. It

29 IANS, "US Warned India Twice of Mumbai Attack by Sea a Month Ago," *Thaindian News*, http://www.thaindian.com/newsportal/world-news/us-warned-india-twice-of-mumbai-attack-by-sea-a-month-ago-reports-lead_100126422.html (accessed 5/18/2009).

30 Christopher Dickey, *Securing the City, Inside America's Best Counterterror Force-the NYPD*, (New York, NY: Simon & Schuster, 2009), 140.

> is also difficult for agencies to accept that they do not have to be self-sufficient but rather can depend on the expertise and data from other organizations to meet their mission. The IC's standard practice of compartmentation and intelligence stovepipes also minimizes information sharing.[31]

The MITRE study does not mean to imply that collaboration intends to necessarily inhibit competitive analysis (i.e., groupthink). As author and intelligence analyst Robert Clark points out, "Collaboration, properly handled, is intended to help competitive analysis by ensuring that competing views share as much information about the target as possible."[32] The collaborative approach also reaches past the traditional customer base of "other intelligence agencies" and draws from operators' perspectives. This expanded view offers two benefits to intelligence analysis: first, it shows or introduces the operator to the value of analysis when dealing with complex issues;[33] second, in a collaborative analytical environment, there is no single point of failure in the "cycle," as the community of interest takes responsibility for the end product.[34]

Studies have shown that culture is the number one barrier in regards to information sharing and establishing trust.[35] Other issues include lack of common goals for collaboration, individual biases and turf battles, system interoperability, and lack of perceived mutual benefit to participate in collaboration.[36]

The National Strategy for Information Sharing states the need for a paradigm shift regarding intelligence practices.[37] This strategy calls for an overhaul of the cold war era structure to one that allows intelligence officials to face emerging threats to homeland security.[38] Additionally, the National Strategy calls on the intelligence community to

---

31 Tamara Hall, Intelligence Community Collaboration Baseline Study, MITRE Corporation (1999) (accessed 5/18/2009).

32 Robert M. Clark, Intelligence Analysis: A Target Centric Approach, 1st ed., 21.

33 Ibid., 20.

34 Clark, Intelligence Analysis, 19.

35 Hall, Intelligence Community Collaboration Baseline Study.

36 Ibid.

37 United States Government, National Strategy for Information Sharing, 1.

38 Ibid.

view the state and urban fusion centers as a valuable information-sharing resource and one that should be incorporated into the national information-sharing framework.[39] The DNI points out in the Intelligence Community Information Strategy that: "…information sharing is a behavior and not a technology."[40] The DNI also notes that the new threat environment forces the intelligence community to review "new national and homeland security customers" in order to sufficiently address the threat.[41] The MITRE study also pointed out that: "To date, most of the initiatives within the IC have focused on the technical requirements to support IC collaboration" without acknowledging that organizational culture is most likely the causal variable in the failure to collaborate.[42] The Department of Homeland Security, while still in its infancy, has realized the value of organizational culture and has invested in a culture of change and collaboration by increasing analytic support and presence in state and local fusion centers around the nation.[43] They have quickly grasped the value of interpersonal relationships in a fused environment. The National Counter Terrorism Center (NCTC), often viewed as the nexus for future collaboration ventures in intelligence, has noted in its information-sharing policy that difficult issues remain, including the ability to share critical information with state, local, and tribal governments and the private sector.[44] While the NCTC has made great strides collectively organizing and sharing across the IC,[45] there are still voids in coverage, and unfortunately, those voids affect the first responders charged with responding to potential threats.

---

39 United States Government, National Strategy for Information Sharing, 1.

40 Office of The Director of National Intelligence, United States Intelligence Community: Information Sharing Strategy, 1.

41 Ibid.

42 Hall, Intelligence Community Collaboration Baseline Study.

43 United States Department of Homeland Security, Department of Homeland Security Information Sharing Strategy.

44 Director, National Counter Terrorism Center, NCTC and Information Sharing: Five Years since 9/11, A Progress Report.

45 NCTC host's counterterrorism community-wide secure video teleconferences (SVTCs) three times daily to ensure broad awareness of ongoing operations and newly detected threats. During these SVTCs, participants compare notes, highlight new threats, and debunk erroneous reports.

D. THESIS OUTLINE AND RECOMMENDATIONS

The first chapter is the introduction and will cover the scope and methodology for this thesis. The second chapter will review the background of the National Maritime Intelligence Center and the transformation process it is currently undertaking. The third chapter will review the underpinnings of trust building by reviewing scholarly work on trust building techniques at the organizational and inter-personal levels. The fourth chapter will review the Joint Inter-Agency Task Force South organization, where trust relationships exist in a collaborative environment. This chapter will attempt to review the theoretical suggestions of scholars on trust, and identify whether trust-building techniques are being implemented in this organization or whether other circumstances have led to successful collaboration within this organization. The final chapter offers conclusions and recommendations for building trust within a collaborative environment.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND—STRUCTURE OF THE NATIONAL MARITIME INTELLIGENCE CENTER AND INFORMATION-SHARING INITIATIVES

A. HISTORY OF THE OFFICE OF NAVAL INTELLIGENCE (ONI)

The Office of Naval Intelligence has served as the epicenter for naval intelligence for over 126 years. As the oldest continuously operating intelligence agency in the United States, ONI has served as the nation's depository for maritime intelligence since its creation shortly after the Civil War. ONI was established to address the decline in maritime intelligence in regards to the capabilities and tactics of foreign navies and in an effort to transition the U.S. Navy into a new era. ONI's mission, at the onset of its creation, was to focus on supporting the modernization needs of the U.S. Navy by providing insight on foreign naval powers' capabilities and the construction methods of their ships. The office was also to serve as a depository for information concerning new tactics and the designs of foreign navies. Secretary of the Navy William H. Chandler, instructed the ONI "to collect, compile, record, and correct information on fourteen categories of naval intelligence."[46] He also envisioned that this information would be readily available to every naval officer.[47]

Shortly after the Civil War, the United States Navy downsized to only a few obsolete ships in comparison to naval powers in Europe. Lieutenant Theodorus Bailey Myers Mason, who was selected to serve as the first commander of ONI, realized the urgent need for the transformation and modernization of the U.S. Navy, and the need for a more robust maritime intelligence center.[48] Mason pressed for "…the creation of an intelligence office to collect and disseminate information on the latest technological developments abroad to support the modernization of the U.S. Navy."[49] Fighting for an

46 Jeffery Dorwart, The Office of Naval Intelligence, the Birth of America's First Intelligence Agency 1865–1918, Naval Institute Press, 1979, 14.

47 Ibid., 15.

48 ONI Web site, Command History, www.nmic.navy.mil (accessed 5/18/2009).

49 Ibid.

official establishment that would focus on naval modernization concerns, the United States Naval Institute was established in 1873, in Annapolis, which served as a semi-official think tank for naval officers to discuss and develop a transformation plan for a new modern navy.[50] Mason served as the institute's secretary in 1879 and helped formulate a prototype office for what would become ONI in 1882.[51] The creation of the office was not widely accepted amongst the other bureaus.[52] Mason noted that the reluctance of other jealous bureaus to share information with the newly established organization ultimately delayed ONI's ability to produce relevant intelligence.[53] Rear Admiral A.G. Berry (Ret.), who was a plank owner of ONI, stated that the new office met with great opposition in its early years.[54] He shared one experience he encountered with the Bureau of Steam Engineering, "The Bureau…had some ordnance notes but refused to give them up, and it required an order from the Secretary to compel that bureau to turn them over to the new office."[55] The lack of coordination and collaboration amongst the bureaus early on was likely, in part, due to the failure of the Navy to consult the other bureaus on the utility and purpose of ONI, thus a lack of trust existed amongst the bureaus and created barriers in information sharing. Mason knew, however, that for the newly established office to be successful and have an impact on naval modernization, the other bureaus must see the value in ONI serving as a central depository of naval information.[56]

While intelligence support for homeland security may seem like a new focus area for ONI, in 1916 Congress authorized and approved budget increases that led to the first major transformation of ONI's role in "supporting domestic security operations, including

50 Dorwart, The Office of Naval Intelligence, the Birth of America's First Intelligence Agency 1865–1918, 8.

51 Ibid., 9.

52 Ibid., 17.

53 Ibid., 18.

54 A. G. Berry, "The Beginning of the Office of Naval Intelligence," U.S. Naval Institute Proceedings, no. 63 (1/1937), 102.

55 Ibid.

56 Dorwart, The Office of Naval Intelligence, the Birth of America's First Intelligence Agency 1865–1918, 18.

protecting America's ports, harbors and defense plants from enemy infiltration, subversion and sabotage."[57] Because of these new intelligence requirements, ONI had to collaborate closely with multiple government bureaus to effectively address this new mission set. Similar to today's transformation, ONI has adapted, since its inception, to address not only foreign naval capabilities, but also national security concerns that affect the homeland.

ONI underwent another transformation with the build-up of World War II. This transformation was brought about due to the need for focused intelligence on both German and Japanese naval capabilities and the development of ways to defeat their navies. During this transformation, ONI became the clearing-house for signals intelligence and photographic intelligence, in support of the war, that ultimately broadened their capabilities and customer base yet again. Additionally, ONI created a schoolhouse for intelligence officers to support the emerging need for timely, relevant, and predictive intelligence in support of operational commanders. Similar to the transition during WWII, the naval intelligence community today is facing a growing demand for actionable intelligence and the desire to reclaim maritime intelligence superiority. Under direction of the Chief of Naval Operations and Director of Naval Intelligence, today's Naval Intelligence Community is attempting to overhaul its sharing and collaborative processes in order to reclaim its role in "information dominance and decision superiority."[58]

From the end of WWII to the end of the Cold War, ONI progressed and transitioned into a center of excellence for operational intelligence and scientific and technical intelligence in support of countering the threat posed by the former USSR. Following the collapse of the Soviet Union and the end of the Cold War, ONI was destined for another transformation that would allow their organization to support both

57 Dorwart, The Office of Naval Intelligence, the Birth of America's First Intelligence Agency 1865–1918, 25.

58 Office of Naval Information, "Transforming Naval Intelligence," Rhumb Lines, Strait Lines to Navigate by, http://www.navy.mil/navco/speakers/currents/Transforming_Naval_Intelligence_27_FEB_09_FINAL.pdf (accessed 1/6/2010).

conventional maritime threats and the emergence of a highly adaptive non-state adversary that has the ability to be both flexible and agile.[59]

Despite several physical moves throughout the D.C. area since its creation in the late 1800s, ONI has continued its intelligence support role for operational commanders. Today the Office of Naval Intelligence operates out of Suitland, Maryland, along with the Coast Guard Intelligence Coordination Center (ICC), which now, under the Department of Homeland Security, plays a key role in supporting domestic homeland security maritime missions by supporting Coast Guard intelligence centers around the nation. The facility continues to expand, with the early 2009 designation from the Director of National Intelligence, as the nationally recognized center for maritime intelligence, which broadens the scope of responsibility of NMIC's traditional role of foreign navy capabilities and white shipping, to a broader reach of maritime concerns, including maritime threats to homeland security.

B. MODERNIZATION AND REORGANIZATION OF ONI

Having realized the need for more defined operational intelligence support for both conventional maritime threats and asymmetric warfare, the Office of Naval Intelligence underwent its latest vigorous restructure in January of 2009, by order of the Director of Naval Intelligence, to better align with the needs of the operators and decision makers.[60] This transition brought about four new centers of excellence to support the Chief of Naval Operations call to restore Naval Intelligence to prominence and dominance:

1. **Nimitz Operational Intelligence Center—**This center is responsible for Maritime Domain Awareness, 24/7 Maritime Operations watch floor and the Fleet and Global Maritime Intelligence Integration. Serving as the central nerve center of the NMIC, this center will play a pivotal role in the NMIC's overall success in building trust amongst its wide array of customers. This center's watch floor is responsible for

59 Wyman Packard, A Century of U.S. Naval Intelligence (Washington D.C.: Department of the Navy, 1996), 145.

60 Office of Naval Information, Transforming Naval Intelligence, 1/6/2010.

identifying and disseminating threat warning indicators within the maritime domain, and also serves as the reporting station for any Maritime Operational Threat Response (MOTR) alerts, which we will discuss in greater detail in the following pages. Identifying and building the relationships needed with first responders who require maritime intelligence will play a large part in building the collaborative environment necessary to address homeland security concerns within the maritime domain. With the expansion of the NMIC and the call by the former Director of National Intelligence to expand the role of ONI, the NMIC was established to orchestrate the MDA process and serve the needs for national maritime intelligence. Because of this unique role of the Nimitz center, this thesis will, in large part, focus on this center of excellence and its adapting role within the global maritime community of interest as well as its role in building a solid trust foundation amongst the maritime community, in order to facilitate smooth communication across a wide-ranging audience.[61]

2. **Farragut Technical Analysis Center—**Focuses on adversary weapons, platforms, combat systems and future technical capabilities.[62]

3. **Kennedy Irregular Warfare Center—**Designed to support a reach-back mechanism for Naval Special Warfare and Navy Expeditionary Combat Command forces.

4. **Hopper Information Services Center—**Established to improve interoperability with information technology by providing a service-oriented architecture.[63]

C. TRANSFORMATION OF THE NMIC AND ITS ROLE IN NATIONAL MARITIME INTELLIGENCE CONCEPT OF OPERATIONS

As previously mentioned, in January 2009, the former Director of National Intelligence, Mike McConnell, declared that the NMIC would serve as the national hub for maritime intelligence. This is largely due to the need for a central nerve center for

61 Office of Naval Information.

62 Ibid.

63 Ibid.

maritime domain awareness and to align with the goals set forth by the president in the National Strategy for Maritime Security, National Strategy for Maritime Domain Awareness, and Global Maritime Intelligence Integration Plan. The NMIC, still in its infancy, faces the daunting task of coordinating and collaborating with over 26 national agencies, in addition to expanding its scope to include state and local homeland security fusion centers with maritime interests.

The National Strategy for Maritime Security laid out eight subordinate plans to support the implementation and coordination processes needed to successfully execute a plan to achieve Maritime Domain Awareness. Former President George W. Bush defined the maritime domain as "All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterways, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."[64] The subordinate plan that lays out the roles and responsibilities of the NMIC and other national agencies is the MOTR plan. The MOTR plan is one of the eight subordinate plans that were implemented to coordinate the threat response processes amongst the U.S. government by identifying and establishing specific roles and responsibilities for all agencies that have maritime responsibility.[65] The MOTR concept of operations was established to coordinate response planning prior to an actual event to avoid confusion and enable national agencies to respond and coordinate against maritime threats in a timely fashion. Within the MOTR plan, the NMIC is designated as the lead agency of the Global Maritime Intelligence Integration (GMII). Identified as a lead agency concerning coordination and collaboration in the event of a maritime threat, the NMIC's responsibilities include, but are not limited to, the following missions:

> Creating and overseeing a collaborative information environment for the global maritime community of interest that informs and guides operational planning and response to ensure the security of the maritime domain… The NMIC core element coordinates its maritime intelligence information

64 The United States Department of Homeland Security, Maritime Operational Threat Response Plan for the National Strategy for Maritime Security, The Department of Homeland Security (2006).

65 Ibid.

> sharing and analytical efforts to become the center of excellence for strategic maritime intelligence analysis and information integration for the U.S. government.[66]

Within the first months of its inception, the NMIC was tasked by the National Security Council to respond to the established U.S. National mechanism for maritime threat response, MOTR plan activation.[67] The timing of the activation coincided with a piracy conference that was taking place at ONI. The former director of the NMIC, RADM Gilbride, was in the process of hosting a conference on international Horn of Africa Piracy that included members of the National Security Council, academics, foreign partners, the maritime industry, and operators to collaborate on effective measures to stop piracy in the region. The conference was originally scheduled to be from 7–8 April 2009 and include key members of the maritime community of interest. On the last day of the conference, the panel and guests were all in attendance when information on the attack of the Maersk Alabama while en route to Kenya to deliver food aid came in. The ship was attacked by four pirates who were unable to take control of the ship. At some point, the pirates realized their attempt to seize the Alabama had failed and fled the ship with the ship's lifeboat and captain as hostage. Within only a few short hours, under the recommendation of the National Security Council and previous Homeland Security Council, the National MOTR plan was activated.[68] In this time of crisis, the conference participants collaborated to support a common goal of rescuing the Captain of the Maersk Alabama. The NMIC took on its role of coordinating maritime policy and coordination throughout the MOTR process. Utilizing the in-house

66 Maritime Operational Threat Response Plan for the National Strategy for Maritime Security.

67 The Maritime Operational Threat Response (MOTR) is an interagency process under National Security Council/Homeland Security Council leadership. MOTR coordinates the response to a wide variety of maritime threats to U.S. security and policy. NMIC is notified that a MOTR call is imminent via the Nimitz Center's Global Maritime Watch. Participation is usually by phone or video conferencing and the nature of the incident determines which agencies participate.

68 Charles Dragonette, "Rescuing the M/V Maersk Alabama, ONI Leadership in Counter-Piracy Analysis," *The ONI Quarterly* (July 2009).

knowledge and the participating members of the piracy conference, the NMIC was able to communicate to a wide-ranging audience throughout the MOTR activation, which lasted eight days.[69]

This unique coordinated response offered a glimpse of the ideal collaborative environment where institutional barriers were not an issue and where a collective whole focused on a unified response to a specific issue. The NMIC was able to quickly capitalize on a shared crisis that created a focused environment where all participants had the same desired end-state. In this event, each organization was also able to realize that a coordinated response was necessary to achieve its goals. As individual organizations, they did not have the manpower or the resources to achieve their desired end-state. In a crisis situation, institutional barriers between organizations are often easier to break for the sake of accomplishing a mission. Having all participants centrally located in the NMIC also supported communication and broke down the traditional barriers of information sharing. The NMIC has the opportunity to capitalize on this experience, but must first understand the factors that made this collaborative event a success in order to apply the findings outside of a crisis management situation. First and foremost, the structure of the NMIC offered the ideal command and control nerve center to effectively coordinate operations and fuse intelligence information between defense and interagency intelligence agencies. Members of the Maritime Community of Interest attending the piracy conference included key stakeholders from all walks of the maritime community. Having subject matter expertise from industry, military, and the interagency on site created an environment where expertise from every field was readily available, and minimized agency barriers that are often present, and prevent collaboration. U.S. Coast Guard Commandant Admiral Thad Allen gave his remarks on the first MOTR response:

69 Participants involved in the MOTR response to the Maersk Alabama include Department of State, Department of Defense, Office of the Director of National Intelligence, CIA, DIA, Department of Justice, Department of Transportation, U.S. Coast Guard, AFRICOM, CENTCOM, NAVCENT, SOCOM, and others.

> Response (MOTR) protocol, a novel concept to orchestrate intra-governmental efforts in maritime incidents, played a positive and significant role. This protocol facilitates interagency unity of effort, efficient information flow and decision-making.[70]

The Maersk Alabama MOTR response is a prime example of the evolving maritime threat environment and the potential for overlapping jurisdictional concerns that require close collaboration amongst the Maritime Community of Interest in order to determine the best course of action. The NMIC's expanding role will require a trust-based foundation to support the collaborative process needed to address maritime domain concerns with precision, similar to JIATF-S's collaborative model that requires multiple agencies to coordinate and respond in a unified effort to combat drug trafficking. A trust-based foundation is a necessity in developing an interagency organization because each agency has information security concerns, different objectives, and organization cultures that must be understood by all participating agencies if a coordinated and collaborative approach is required. The JIATF-S model has been viewed by many in the interagency as the gold standard for interagency collaboration and will be discussed in detail in the following chapters.

To address the growing demand for maritime intelligence, both in crisis situations and everyday coordination, the NMIC will need to establish a trusted environment for interagency partners to operate in effectively.

While the first MOTR response is viewed by the participants as a success, creating an organization that incorporates the expertise from a wide range of agencies requires time and patience to establish credibility, acceptance, and most importantly, trust, to operate in a coordinated manner on a day-to-day basis.

The ONI centers of excellence, which support the NMIC, have built a strong reputation for their naval intelligence support for tactical, operational, and strategic leadership for quite some time. The 24/7 Nimitz watch floor serves as an avenue for naval leadership to tap into at anytime to address issues that arise and receive intelligence

70 Anthony Russell, "Statement by Adm. Thad Allen, Commandant of the Coast Guard, on Piracy," United States Coast Guard, http://www.piersystem.com/go/doc/786/268323/ (accessed 1/6/2010).

support. The fact that ONI is the longest serving intelligence agency, and has evolved over time to support mission commanders, solidifies the newly established NMIC's mission of expanding maritime intelligence to a much wider audience. The trust foundation ONI has built, as a competent supplier of naval intelligence, will play a critical role in establishing the trust environment needed within the NMIC for interagency partners to operate in. The NMIC has the opportunity to capitalize from the success of its first MOTR plan response by continuing to find effective ways of communicating within the inter-agency, and by creating a culture within the NMIC that focuses on collaboration and critical trust building methods that will be discussed in Chapter III.

D. NATIONAL INFORMATION-SHARING EFFORTS BY THE DIRECTOR OF NATIONAL INTELLIGENCE (INFORMATION SHARING ENVIRONMENT)

For the NMIC to create a trusted collaborative environment, it requires the proper structural foundations and doctrine to support a culture shift within the IC. The 2004 Intelligence Reform Act created both the position of the Director of National Intelligence and the call for establishing an Information Sharing Environment to address a major shortfall cited in the 9/11 Commission Report. Along with the 9/11 Commission's findings, several other studies have also cited a lack of information sharing within the intelligence community and the need for intelligence reform (see Figure 1). Since the ISE's inception in 2005, The ISE Manager has stated, "exceptional progress has been made to implement the ISE nationwide." This initiative is a drastic change in the intelligence community's culture and has taken an exceptional amount of work to implement the processes necessary to move in the right direction. In the 2009 ISE annual report to Congress, the initiative transitioned from implementation to developing the framework to support the "most developed information-sharing environment in government to date."[71]

71 Thomas McNamara, *Information Sharing Environment, Progress and Plans, Annual Report to the Congress* (2009).

	9/11 Commission	Markle Foundation	Government Accountability Office	WMD Commission	National Strategy for Information Sharing
					
FOCUS	Examined failures in uncovering the 9/11 plot owing to poor information sharing across agency boundaries	Studied the nature of information sharing with an emphasis on decentralized, trusted networks	In several reports, assessed progress toward improving information sharing in intelligence, homeland security, and critical infrastructure	Analyzed the sharing and analysis of intelligence leading up to the second Iraq War	Delivered a fully-coordinated Federal, State, local, and private sector strategy, identifying specific outcomes to improve terrorism-related information sharing
MAJOR RECOMMENDATIONS	• Provide incentives that promote information sharing • Bring U.S. national security institutions into the information revolution • Create decentralized, trusted information networks across the Federal government	• Build a networked community for homeland security • Reduce gaps across Federal agencies and with state and local government and the private sector • Create horizontal information sharing and integration	• Information sharing is a "High Risk Area" for the U.S. Government • Improve coordination across information sharing initiatives • Improve Federal-state-local arrangements • Adopt a comprehensive set of performance measures	• Create a single focal point for information sharing under DNI • Establish uniform standards and break down policy and technical barriers • Expand sharing of all intelligence, not just terrorist-related information	• Foster a culture of awareness • Weave information sharing into all aspects of counterterrorism activity • Implement procedures, processes, and systems that draw upon and integrate existing technical capabilities and established agency authorities

Figure 1. From 2009 Annual Report to Congress, Information Sharing Environment[72]

The ISE framework is built around four functional areas—creating a culture of sharing; reducing barriers to sharing; improving sharing practices; and institutionalizing sharing.[73] Sharing information, however, requires a great deal of trust amongst participating organizations. Creating a framework that institutionalizes "sharing" will only succeed if the underpinnings for collaboration exist. The ISE framework at the organizational level, institutionalizing sharing practices will create a standard to measure progress within the organization and against other organizations. The idea of openness and reciprocity within a shared environment are key elements to building trust at the

72 McNamara, *Information Sharing Environment, Progress and Plans, Annual Report to the Congress* (2009).

73 Ibid.

organizational level and will be discussed in detail in the following chapter. The ISE framework proposed has the potential to support the change in culture within the IC if the proper steps are taken to understand how trust develops amongst organizations. If the foundational issues of trust building are not institutionalized within the ISE's efforts, organizations will work around loopholes in information sharing. The ISE has developed what they call the maturity model concept to assess progress in information sharing over time (see Figure 2). Understanding your desired end-state is step one in developing any strategy to achieve your desired end-state. If the goal is to institutionalize information sharing and collaboration, then building a network and environment that supports trust building is a critical step in achieving a shared environment. The ISE's efforts to create a structure that can facilitate collaboration is not the end-all answer to solving stove-piped systems, but it does help dissolve bureaucratic walls that have traditionally blocked collaboration from agency to agency. The Information Sharing Environment is an IC-wide initiative that requires a complete culture change from the way the IC has traditionally viewed intelligence and the way it has conducted business.

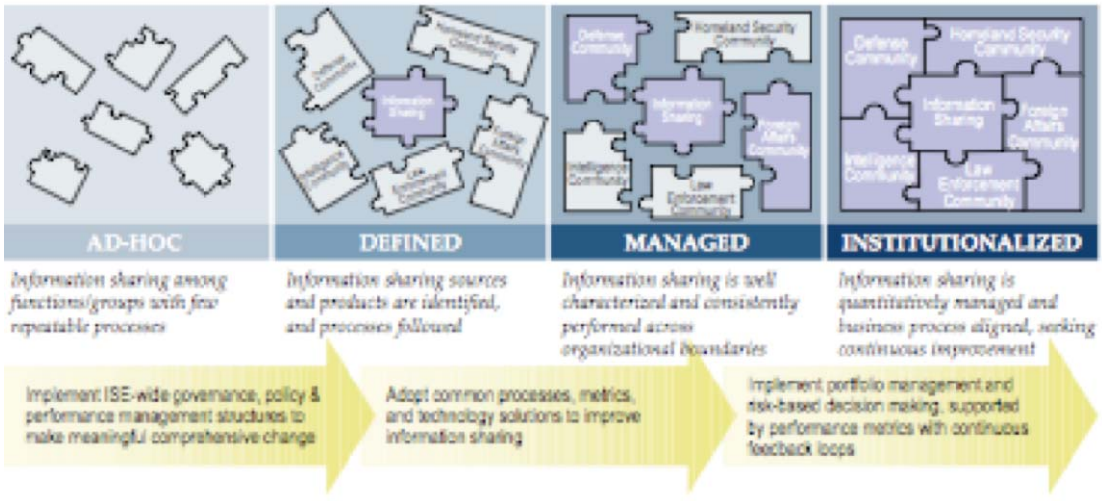

Figure 2. From Annual Report to Congress, ISE Maturity Model Concept[74]

74 McNamara, *Information Sharing Environment, Progress and Plans, Annual Report to the Congress* (2009).

E. MARITIME DOMAIN AWARENESS CONCEPT OF OPERATIONS IMPLEMENTATION AND THE ROLE OF TRUSTED RELATIONSHIPS

The goal of achieving maritime domain awareness cannot come to fruition if a trust bond is not created amongst the various agencies responsible for implementing the MDA Concept of Operations (MDA CONOPS). This plan references several shortfalls in creating a collaborative network of trust across agencies, to include, "lack of trusted partnerships," "incorrectly perceived policy restrictions on sharing data," and "limited interagency communications."[75] The MDA CONOPS weighs trust as a critical element in the overall success of MDA:

> Effective Intelligence and information sharing is critical to understanding the maritime domain and improving safety and security of the United States. For information sharing to succeed, there must be trust—the trust of information providers, the users of information, policymakers, and most importantly of the public. Each of these must believe that information is being shared appropriately, consistent with law and in a manner protective of privacy and civil liberties.[76]

The MDA CONOPS is structured around identifying key "Enterprising Hubs" to assume responsibility for certain functional areas (see Figure 3).[77] The plan's architecture is based around specific agencies' "respective area of expertise" and assigning coordination responsibilities for specific fields (e.g., vessels, cargo, people, infrastructure, and architecture management).[78] Unless trusted relationships that will support the implementation of this CONOPS are built, the plan will never reach its full potential. The enterprising hubs cover a wide range of agencies that do not necessarily have a well-defined working relationship. Understanding the factors that go into building and managing trusted relationships will ultimately support the NMIC's expanding requirements as an agency lead in MDA and the DNI's goal of openness and a

75 The United States Department of Homeland Security, National Concept of Operations for Maritime Domain Awareness, (2007).

76 Ibid.

77 Ibid.

78 Ibid.

responsibility to provide, within the intelligence community at large, and include the expanding domestic Homeland Security mission that has not traditionally benefited from national intelligence agencies.

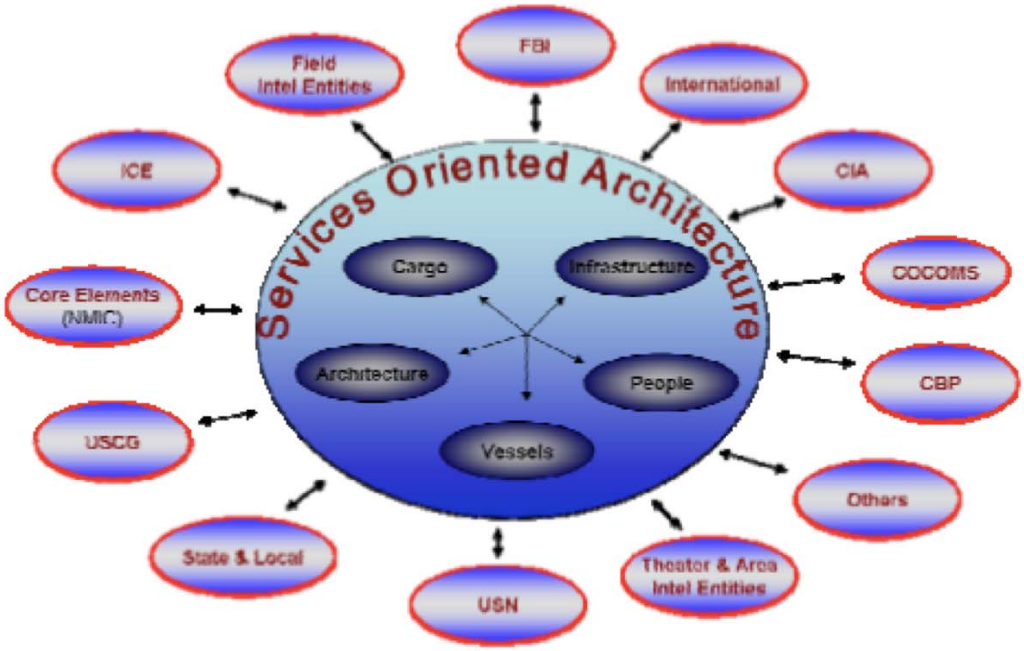

Figure 3. From the National Concept of Operations to Achieve MDA, Enterprising Hub Structure[79]

These three endeavors call into question: how do you successfully build trust? What are the critical factors that support the establishment of a trusted relationship amongst such a wide-ranging audience, which demands different requirements and needs to satisfy each organization's intelligence? As important as understanding the critical factors of building trust, what are the factors that will cause trust to break amongst organizations? Understanding the ramifications of lost trust is just as important as building trust because lost trust could impede future collaborative efforts and negate any efforts of collaboration in the future. The following chapters will try to address these very issues and identify what scholars have noted as the key factors of building trust.

79 National Concept of Operations for Maritime Domain Awareness.

These three endeavors are all intertwined and require multiple agencies' support and contribution for each to be successful. Identifying what works in trust building, as well as what does not work, will ultimately provide a strategy that can focus limited resources in the right area in order to achieve maximum benefit and return in order to build a collaborative environment that supports all three.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE DEVELOPMENT OF TRUST IN COLLABORATIVE NETWORKS

Organizational and interpersonal trust has been identified as a pivotal success factor for collaboration in both the private and public sectors. This chapter will focus on the underpinnings of collaborative team trust building. It will review current practices, literature, methodology, and the outcomes of trust building. The chapter will also attempt to extrapolate common trust threads throughout the trust literature in order to understand their significance in building a trusted environment. Additionally, this chapter will recommend specific actions for building inter-agency collaborative trust.

Proposed is a structural and inter-personal model for trust building in any inter-agency setting that requires relationships with agencies from various backgrounds. Integrating trust building into an organization's environment has the potential to support the NMIC's expansion into domestic intelligence support for Homeland Security as well as their conventional maritime intelligence support role. In today's threat environment, it will become crucial for agencies to collaborate in order to maximize threat warning and reach all intended customers. Collaborative initiatives take place so that collaborating agencies can achieve a set end-state or goal that they could not achieve individually.

The NMIC has a unique opportunity to take advantage of various agencies' expertise in today's dynamic operating environment that often requires a collaborative environment. In this era of inter-agency cooperation, how do organizations develop the relationships and trust that is necessary to successfully operate and accomplish a wide range of mission sets?[80] The general literature regarding building trust amongst organizations with different cultures, missions, and capabilities suggests there are key structural formulations that are most likely to lead to effective trust relationships between

80 Piotr Sztompka, Trust: A Sociological Theory (Cambridge: Cambridge University Press, 1999). 25. Trust is defined in this paper in accordance with Sztompka's definition of trust essentially being, "a bet about the future contingent actions of others."

such organizations. Are these structural formulations being applied effectively according to the recommendations of trust theory between national intelligence organizations and inter-agency partners?

Based on a review of the general trust literature, there are several principles that can be considered essential to developing trust. When organizations work together, trust relationships are made up of two fundamental relationships: inter-personal and organizational. Inter-personal trust is discussed in great length by authors such as Stephen Covey. In Covey's discussion of trust, he outlines four core competencies of trust: "1) Integrity: Are you Congruent? 2) Intent: What's your agenda? 3) Capabilities: Are you relevant? and 4) Results: What's your track record?"[81] Each of these core competencies must be exuded in each inter-personal relationship to truly facilitate trust within an organization.

While principles such as Covey's are critical for maintaining an overall sense of trust within an organization as a whole, organizations may require additional means of developing trust. At a structural level, however, there are more strategic recommendations for managing trust within an organization. Trust scholars such as Andrew Van de Ven and Peter Smith Ring argue that there has been a significant shift within modern society from interpersonal trust to a reliance on institutional trust.[82] Their claim echoes those of L. G. Zucker who is cited by several authors for his research on the evolution of trust in American society from one of interpersonal relationships to one reliant on institution-based relationships.

Zucker's 1986 studies indicated that there were two distinct means of structuring an organization to build trust: informal structure or formal structure—social interactions may be enough to generate trust if a project is temporary; however, a long-term project

81 Stephen Covey, *The Speed of Trust, the One Thing that Changes Everything* (New York, NY: Free Press, 2006). Intent 73–90. Capabilities, 91–108. Results, 109–124. When trust doesn't exist, Covey warns that there are seven general 'taxes' that are placed on an organization: 1) redundancy. 250, 252, Bureaucracy 250–251 3) Politics, 251, 254 Disengagement, 251, 255 Turnover, 252, 256 Churn, 253, 257, Fraud, 253.

82 Andrew Van de Ven & Peter Smith Ring, "Relying on trust in cooperative inter-organizational relationships," In Handbook of Trust Research. Ed. Reinhard Bachmann & Akbar Zaheer (Northampton, MA: Edward Elgar, 2006).144–164, 145.

may require bureaucratically guided, procedure-based interactions to "[assure] consistency."[83] Social networks can also be replaced with formal processes and procedures codified into the network — the higher level of institutional based trust, as developed from these bureaucratically guided procedures, the lower the need for inter-personal trust to successfully operate.[84] Zucker notes that, "from the institutional perspective, organizational structure may be less a means of organizing for efficient production and more a means of generating trust."[85] Van de Ven and Ring argue that trust can be supplanted at the organizational level by "relational quality…reputation…and legitimacy."[86]

To further generate trust within and amongst these institutions, scholars have several recommendations. Sztompka notes the importance of structure in eliciting trust in his analysis of the effective organization of an entity.[87] In order to create trust, he articulates five critical structural contexts that must be present: 1) normative coherence, 2) stability of the social order, 3) transparency, 4) familiarity, and 5) accountability.[88] Consistent and coherent legislation must codify these values.[89] To further the structural mechanisms for trust, Sztompka notes that there are contextual methods of facilitating trust as well: encouraging accountability, pre-commitment, and situations that require reciprocal trust.[90]

---

83 William Stevenson, "Organization Design" Handbook of Organizational Behavior, 2nd ed. Ed Robert T. Golembiewski (New York, NY: Marcel Dekker, Inc., 2001.) 145–174.

84 Stevenson, "Organization Design," 162. & Van de Ven, "Relying on trust in cooperative inter-organizational relationships," 150.

85 Ibid., 145–174, 162.

86 Van de Ven & Ring, "Relying on trust in cooperative inter-organizational relationships," 153.

87 Sztompka, Trust: A Sociological Theory. He describes different structures of cooperation that affect trust. He notes that "mechanical solidarity" allows individuals to work at similar tasks separately, but towards a common goal (Sztompka, 63). When conducted through parallel efforts, this mechanical solidarity can lead to sub-par, but equal performance (Sztompka, 64). "Organic solidarity" requires cooperation and coordination in which the successful performance of specialized tasks is required (Sztompka, 64).

88 Ibid., 122–124.

89 Ibid., 134.

90 Ibid., 87, 91, 93.

To balance the general trust literature, much of the inter-agency critiques focus on the difficulties of relying on such structural formations to create trust and facilitate successful operations. James Carafano warns of the U.S. repeating history in its inter-agency reforms, specifically the dangers of ignoring the significance of human interaction and relying on the bureaucratic structure to develop trust.[91]

Uniquely, while Americans in general are becoming more and more distrustful of one another, the U.S. military continues to enjoy high levels of trust.[92] In his analysis of the military's development of trust with the general public, David King and Zachary Krabell argue that successful military performance (internal reform and successful high profile military operations such as Grenada and Panama), professionalism (end of the draft, racial integration), and effective use of its symbolic power since the 1970s has engendered public trust.[93] The U.S. military also aligns with Sztompka's analysis of the three means of judging trust within an initial interaction: reputation, performance and appearance.[94] In these categories, the military may engender more trust than other agencies due to its successful reputation (credentials and competence), performance ("actual deeds"), and appearance and demeanor (uniforms, fitness, manners, marketing).[95]

In spite of arguments that the U.S. military has generated trust among the general American public as a competent organization, it has an arguably blemished history in the realm of inter-agency operations in generating trust. Due to its difficult history with inter-agency operations, the Joint Chiefs of Staff issued in 1996, and again in 2006, the Joint Publication 3-08 offering guidance on how the U.S. military should interact with other

91 James Jay Carafano, "Interagency Dialogue: Managing Mayhem: The future of Interagency Reform" Joint Forces Quarterly. Issue 49, 2nd Quarter 2008. 135–137. Carafano warns that the bureaucratic structures cannot "overcome operational inaction." 135.

92 Van de Ven and Ring, 155. David King & Zachary Krabell. The Generation of Trust: Public Confidence in the U.S. Military Since Vietnam. (Washington D.C.: The AEI Press, 2003).

93 King & Krabell. The Generation of Trust:. 8, 13, 20–31, 32–69.

94 Sztompka, 71.

95 Ibid.

agencies.[96] It offers guidance similar to that suggested by the aforementioned trust scholars. Mainly, it provides insights into how the military should perceive the inter-agency context to facilitate trust: coordination and planning must be done outside of the context of military command and control, and, other agencies must rely primarily on "perceived mutually supportive interest" to develop relationships rather than formal authority.[97] Unified goals must be achieved and must develop functional interdependence.[98] Others scholars offer still more specific guidance with respect to inter-organization operations. The Critical Infrastructure Protection report on "Public Trust" argued that a clear communications chain was paramount to inter-agency success.[99]

Following a thorough review of the trust literature, the remaining portion of this chapter will attempt to identify the consistent trust themes that carry over from various disciplines in order to identify the key factors that support a trusted relationship and offer a foundation for newly established organizations like the NMIC to explore and utilize. Trust is dynamic and can change over a period of time.[100] Trust is not as simple as "yes, I trust someone" or "no, I don't trust someone." Trust operates on multiple layers and this chapter will attempt to separate trust relationships into what has been identified as the three common themes of trust: competence trust, ethical trust, and emotional trust.[101] This concept is similar to Covey's two-part trust composition of character and competence trust. Romahn's model, however, separates emotional and ethical trust from character trust as ethical trust is based upon the trustor's expectations of any given

96 Joint Publication 3-08. "Interagency, Intergovernmental, Nongovernmental Organization Coordination During Joint Operations Vol. I." 3/17/2006. www.js.pentagon.mil/doctrine/jel/new_pubs/jp3_08v1.pdf (accessed: 09/28/2009).

97 Ibid., 20.

98 Ibid., 24.

99 Lee M. Zeichner. "Legal Foundations: Public Trust and Confidence in Critical Infrastructure." The CIP Report. May 2006. Vol. 4, No. 11. 3–4 & 13, 4.

100 Elke Romahn and Francis Hartman, "Trust: A New Tool for Project Mangers" (Philadelphia, Pennsylvania, October 10–16, 1999).

101 Ibid.

situation and may not involve or require any emotional relationship with the trustee.[102] Additionally, high and low levels of emotional trust can dominate and falsify the other categories of trust, thus the need to create a specific category for emotional trust.[103]

Some element or resemblance of competence trust is the most dominant thread throughout the literature on trust, and probably, once established, is the most stable form of trust overall. This form of trust builds upon ability, performance, and track record for a specific job or tasking. Building competence trust is at the foundation of building a solid trust relationship, both personally and within an organization, because it requires proof of ability in a specific field, especially when a new relationship is being formed without any previous interaction or experience. There is little difference in the business world. As Covey points out, people want to know about your results because this helps establish some level of competence in any given field.[104]

The second common thread of trust identified is ethical trust. Ethical trust is built upon expectations that either an individual or organization's interests will be taking care of.[105] Rohman states, "Ethical trust is based on the trustor's expectations and how well they are being met."[106] With that said, it is essential to have a clear understanding of the expectations for all organizations contributing to the collaborative network and knowing that these expectations may change over time. This is a critical factor in supporting a collaborative relationship. Clear communication of expectations will prove essential to building ethical trust and avoiding a collapse or breakage, either intentionally or unintentionally. Once ethical trust is broken, it is extremely difficult to regain, if at all. Any organization attempting to build a collaborative network must also understand that the expectations for each participating organization will most likely be different. Understanding the needs for specific information will avoid costly miscalculations and time-consuming efforts for nothing. In addition to expectations, one must also

102 Covey, *The Speed of Trust, the One Thing that Changes*, 110.

103 Romahn and Hartman, Trust: A New Tool for Project Mangers, 4.

104 Covey, *The Speed of Trust, the One Thing that Changes Everything*, 112.

105 Romahn and Hartman, Trust: A New Tool for Project Mangers, 3.

106 Ibid.

understand the capabilities of each organization. A good example is the U.S. Navy carriers' bandwidth capabilities. Compared to the cruisers' and destroyers' communication capabilities, it is like night and day. If the carrier's intelligence center is responsible for providing intelligence support for its escort ships, sending large PowerPoint briefs and bandwidth-intensive products over e-mail is not understanding your customer's needs and limitations. The Independent Intelligence Specialist, Executive Officer, and Command Officer aboard the escort ships will likely receive the products late, or not at all, due to the size limitations. This in turn sends the message that their intel needs are not a priority and are not being taken into consideration. This leads to a break in ethical trust across many different channels. Clear communication and understanding of the expectations and capabilities of your partners will support an ethical trust environment. If all collaborative partners feel their needs are being met and considered, the likelihood of reciprocal trust will develop.

The last trust type identified is emotional trust, which varies by situation and can go from one extreme to another.[107] Emotional trust can stem from values and other influential cultural aspects.[108] Emotional trust is desired, however, like anything else, a balance is needed. Extremely high levels of emotional trust can often blind the more concrete aspects of competence and ethical trust. One example of an extreme low in emotional trust would be an organization blaming the CIA for the failures of 9/11, accusing it of mishandling information and providing no value to national security. That organization would be focused on one issue and completely ignore the complexity of an organization the size of the CIA and all the accomplishments it has made in the past. This is an example of extremely low emotional trust, however, emotional trust, unlike the other two trust types, can go from one extreme to another. If the CIA was acknowledged for successfully thwarting an attack, their emotional trust value would likely rise in the eyes of that same organization.

107 Romahn and Hartman, Trust: A New Tool for Project Mangers, 3.

108 Ibid.

Having identified the common threads of trust across the literature, the next step will be to identify how these trust types function and develop over time. The most important element to point out is that the trust relationship is ultimately dependent upon the collaborative group as a whole. The desire to have a trusted relationship must be present to support growth in new areas. Chief of Naval Operations Admiral Roughead says, "Trust, personal trust, is indispensable to partnerships of any kind. … Trust cannot be surged."[109] Rohman points out that the trustor/trustee relationship is built upon each side displaying either trusting or trustworthy behavior, depending upon the situation and the role each organization is playing at any given time.[110] The trustor/trustee relationship is said to reach maximum effectiveness and utility when both trusting and trustworthiness are high (all three levels of trust types are high), but not extreme.[111] Any other combination is viewed as inefficient and possibly damaging to future collaboration (see Table 1.).[112]

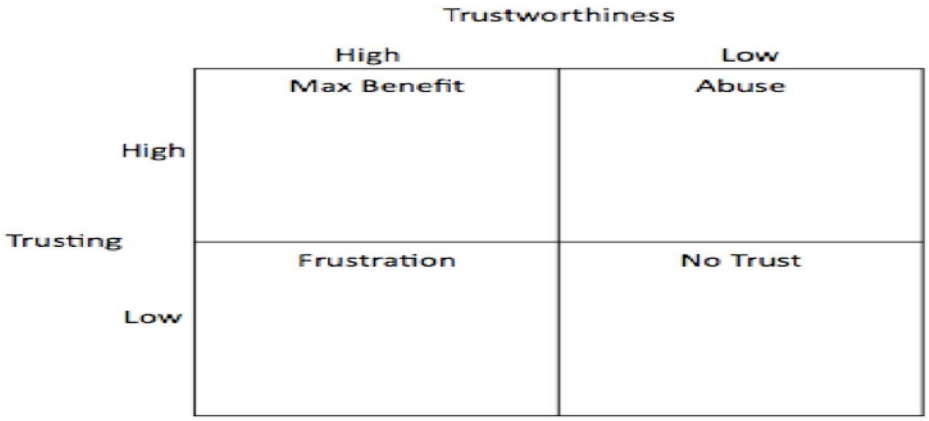

Table 1. From A New Tool for Project Managers, Understanding the Need for Both Trusting and Trustworthiness Relationships[113]

109 Chief of Naval Operations Adm. Gary Roughead Delivers Remarks at the 19th Biennial International Seapower Symposium October 7, 2009.

110 Romahn and Hartman, Trust: A New Tool for Project Mangers, 4.

111 Ibid.

112 Ibid.

113 Ibid.

The next chapter will attempt to analyze inter-agency relationships between the U.S. military and other U.S. government and private sector agencies to identify the structural formulations and inter-personal relationships that should exist to build trust. The author put specific emphasis on whether the theoretical suggestions of scholars on trust are in any way being implemented between these organizations. It will be difficult to prove whether the U.S. military and inter-agency organizations are successful at building trust between each other, which is why this thesis focuses on the analysis of the adequacy of the structures put in place that will most likely lead towards trust building. Where appropriate, the author will provide judgment as to whether the theoretical models are actually having the results they predict based on anecdotal evidence and personal experience.

Having identified the common threads within the trust doctrine, the following chapter will attempt to understand whether these three trust types have played a role in the success of the collaborative environment developed within the JIATF-S organization in order to understand whether they can be applied effectively within the newly established NMIC. Chapter IV will review the following questions, and attempt to answer them based on anecdotal evidence and past experiences, in order to understand whether the three common trust threads of trust development identified have had an impact on the success of these organizations. The following questions will help reveal the impact of the common trust threads in order to understand their utility in building trusted collaborative environments within the following cases:

Does your organization show drive in finishing a task or project or finding an answer to a complex problem? Trust will run low if the organization's overall mission does not match up with the actions by its employees. Action will support trust building and will build confidence in the overall level of competence of the organization as a whole.

Does your organization practice openness in regards to information sharing? Withholding information amongst departments and other collaborating organizations will often lead to a break in ethical trust—which is almost always irreversible.

Is the command leadership in line with the mission of the organization? Consistent and reinforced behavior from the leadership will ultimately support competence trust by supporting a constructive environment that aligns mission objectives with information sharing efforts; what I say is what I do.

Are there methods in place to provide feedback to both consumer and provider in order to better answer the needs of the collaborative whole? This will support ethical trust because both the trustor and trustee will see that their needs drive the production process. Additionally, clear communication is the key factor for keeping emotional trust stable and for avoiding any breakage in the collaborative relationship.

IV. A TRUSTED COLLABORATIVE ORGANIZATION (JIATF-S) AND A FAILED COLLABORATIVE ENVIRONMENT (NOVEMBER 2008 MUMBAI ATTACKS)

The following chapter will review the development of trust in the JIATF-S organization and how that trust bond is pivotal to the development of a successful collaborative environment, on both the organizational and inter-personal levels. This chapter will look at the applicability of the three common threads of trust identified in the previous chapter and will review how JIATF-S, in their own unique way, has applied specific trust concepts in order to effectively build a successful collaborative environment. Additionally, this chapter will review the failure of trust, integration, and collaboration that took place in Mumbai, India in November of 2008 in order to understand the pitfalls of distrust within a non-collaborative environment.

The necessity for interagency collaboration in the United States Intelligence Community has never been greater, thus there is a need to try to understand the ideal environment needed to build trust in inter-agency organizations. It has become increasingly apparent, in an asymmetric threat environment, that coordination amongst intelligence organizations is essential to prioritize the work, minimize duplication, follow suspected threats, and corroborate multiple data sources in order to respond to specific threats with unified action. This thesis is not arguing that inter-agency coordination is easy by any means. Coordination within an inter-agency environment faces the daunting tasks of blending cultural biases, agency norms and functions, and specific ways of doing business. This process is extremely difficult and it requires a continuous cycle of development, nurturing, and transformation to reach its efficacy of true inter-agency coordination. The relationships that are established early on will ultimately define the utility of an inter-agency organization. This chapter will attempt to show how trust development within JIATF-S has supported the collaborative environment that has matured over time, and how trust building is a critical factor for responding to the dynamic threat environment that exists today.

A. JOINT INTERAGENCY TASK FORCE—SOUTH (JIATF-S)

While there is obviously already a long-standing history of maritime intelligence within ONI, there are lessons to be learned by other agencies that have adapted and practiced inter-agency coordination within the maritime realm, which are considered by many in the inter-agency to be extremely successful. This chapter will review the development of JIATF-S and its inter-agency design. Established in 1994 in Key West, Florida as a counter-drug tool, JIATF-S has become a model for inter-agency organizational design due to its ability to streamline information and break down institutional and international barriers that once crippled a quick response to narco-traffickers.

Subordinate to USSOUTHCOM, JIATF-S is unique in its design as it is manned by members from all U.S. service branches and the following U.S. government agencies: ONI, DHS, DEA, FBI, NSA, NRO, CIA, and NGA. The thirteen foreign agencies represented at JIATF-S include: Argentinean Air Force, Brazilian Agency, Colombian Air Force and Navy, Ecuadorian Air Force, French Navy, Mexican Navy, Royal Netherlands Navy, Peruvian Air Force, UK Royal Navy, Spanish Guardia Civil, and Venezuelan Air Force.

With this wide assortment of different organizations and nations within JIATF-S, the needs of each organization vary, but the mission of JIATF-S is clear and succinct. Ultimately, it supports the focus and the goals of the organization overall and enables multiple organizations to converge on the unified issue of narco-terrorism.

JIATF-S aligns its operations, intelligence fusion and multi-sensor correlation on narco-trafficking targets. It detects, monitors, and then hands off these targets to law enforcement agencies or the military. A typical mission sequence encompasses a carefully orchestrated series of handoffs that begins with interagency intelligence collection, then flows to military detection, sorting and monitoring of events, and concludes with the transfer of responsibilities for interception, arrest and prosecution to the law enforcement community. JIATF-S also promotes security cooperation through counterdrug engagement with host nations and supports country team and partner nation

initiatives on foreign soil. Throughout its efforts, JIATF-S focuses on terrorist organization involvement in the drug trade as a means to further terrorist activities.

1. Mission Focus and Alignment Within JIATF-S

In the early stages of developing JIATF-S, Department of Defense (DoD) leaders were particularly keen on establishing an interagency task force to synchronize U.S. government actions against narco-trafficking. Nevertheless, multiple agencies had concerns that such a task force might delay, rather than facilitate, the flow of counter-narcotic information. As the task force matured, three attributes contributed most to its effectiveness: a shared vision of the importance of its task, location in a single command and control space, and the shared experiences of its members.

JIATF-S mission, vision and goals are defined and serve as the backbone to mission development within the task force and create a unified response from the various agencies within JIATF-S. This task force was designed around the shared idea and focus that the problem of illegal drug flow was too large for any one organization or nation to take on unilaterally, therefore, the requirement for a more robust inter-agency counternarcotics organization was needed to combat drug trafficking.

Prior to the creation of the Joint Task Force, the United States Coast Guard carried the major responsibility of responding to and interdicting narco-traffickers, however, with limited assets, and poor coordination and relations between disparate agencies, the well-funded narco-traffickers would often go unscathed.[114] A custom official even notes, "Back then, Coast Guard and Customs service air stations refused even to coordinate flight schedules or patrol grids to avoid useless duplication of effort."[115] Miami Air Branch Chief Robert Viator is amazed at the transformation that has taken place over the last decade, recalling the establishment of a combined Customs and Coast Guard air operations center prior to the establishment of JIATF-S. Viator witnessed the ribbon-cutting event where the customs commissioner broke ground

114 James Kitfield, "Anti-Drug Task Force may Provide Homeland Security Blueprint," *National Journal* (2002), http://www.govexec.com/dailyfed/0902/092002nj1.htm (accessed 1/15/2010).

115 Ibid.

followed by the Coast Guard commandant shoveling the dirt back into the hole made by the customs commissioner.[116] Viator claims he overheard the Coast Guard commandant say, "Whatever you do, I can undo!"[117] What was once the predominant way of conducting business in counter narcotics has slowly faded away with the realization that narco-trafficking is an epidemic and each agency has limited assets to bring to the fight. Turf battles and stove-piped organizations were, therefore, counter-productive. The goal became the merging of the capabilities of each agency and nation and the breakdown of barriers between agencies to provide a unified response to narco-trafficking.

The evolution of JIATF-S has provided many lessons. First, it highlights the types of challenges that organizations with diverse and sometimes conflicting missions face in integrating efforts to address a complex and dynamic problem. Some of these challenges—the need to establish confidence in the new group's ability to participate, and define roles and relationships—are consistent with those found in other inter-organizational groups in both the public and private sectors. JIATF-S has succeeded in identifying and focusing its mission, supporting all of the partner agencies and nations contributing to a common goal. By doing so, JIATF-S has "…target[ed] specific missions and clearly defined their objectives, to include detecting, monitoring and targeting narco-terrorists and the drugs they profit from."[118] Because each agency within JIATF-S has a vested interest in achieving these objectives, the collaboration and openness of the unified response has proven to be successful in aligning the necessary resources from each agency to combat this difficult issue.[119]

The following mission, vision, and goals of JIATF-S were designed to support the collaborative whole by building a unified front where trust is paramount:

116 Kitfield, "Anti-Drug Task Force may Provide Homeland Security Blueprint."

117 Ibid.

118 Richard Yeatman, "JIATF-South, Blueprint for Success," Joint Forces Quarterly, no. 42 (2006).

119 Ibid.

> JIATF-S Mission—Conduct interagency operations against illicit trafficking by highly mobile asymmetric threats originating or transiting its joint operating area by detection and monitoring of illicit air and maritime targets, intelligence fusion, information sharing, and multi-sensor correlation to facilitate interdiction and apprehension along with partner nations in support of national security and regional stability.
>
> JIATF-S Vision—JIATF-SOUTH will be the center of excellence for all-resource fusion and employment of joint interagency and international capabilities to eliminate illicit trafficking posing a threat to national security and regional stability
>
> JIATF-S Goals—Eliminate the primary flow of illicit drugs in and through the joint operating area. Expand to include all critical international and interagency partners. Achieve 100 percent domain awareness of illicit trafficking. Shape the command for success.[120]

Development of a unified mission statement aligns each contributing organization to a specific cause and illustrates the types of decisions and actions that each participating agency will have to take to create the cooperative processes and the required communication necessary to be successful in creating a collaborative environment. Trust scholar Markus Schobel finds that in high-reliability organizations, "Trust can be further based on perceived value congruence between trustor and trustee."[121] Therefore, in a time of crisis, or even day-to-day operations, "[Partners] will approach...situations in a way that is consistent with the general thrust of one's expectations."[122] If each organization contributing to the inter-agency process understands the mission objectives and also feels they had a key role in developing the mission objectives, then a unified response, built around trust, will most likely develop.

Each organization participating within JIATF-S has the expectation that their needs are being supported by the collaborative whole through this unified mission. If this mission is achieved, its success provides the ideal environment for ethical trust to flourish by building a trust foundation through actions and reciprocity. Task force officials admit

120 SOUTHCOM Command Web site, http://www.southcom.mil/PA/facts/CmdOrg.htm (accessed 1/26/2010).

121 Markus Schobel, "Trust in High-Reliability Organizations," Social Science Information 48 (2009), 315, http://ssi.sagepub.com/cgi/content/abstract/48/2/315 (accessed 1/26/2010), 318.

122 Ibid., 319.

that it has taken years "and many acrimonious cultural clashes" to build the trust environment that exists today at JIATF-S.[123] JIATF-S is not an overnight success by any stretch. The trusted relationships that have been developed require constant nurturing and open communication amongst the stakeholders. Intelligence Analyst Robert Clark refers to this as "sharing soft information" with the collaborative whole to build rapport, such as sharing "ideas, questions, problems, objections, opinions, assumptions and constraints."[124]

Additionally, the legal underpinnings and agreements between the interagency and international partners provide the structural foundation and evidentiary support that each organization requires in order to operate within a defined trusted environment.[125]

2. Information Sharing Within JIATF-S

Information sharing is by far the most critical element within the JIATF-S organization. Without timely and actionable intelligence dissemination to the proper authorities, the command would be rendered useless. JIATF-S is a DoD command, therefore the military personnel within the command cannot serve as law enforcement personnel and interdict and arrest narco-traffickers suspected of illicit activity. Information sharing is critical to the task force because it enables law enforcement personnel to act on actionable intelligence in a timely fashion. Having built a level of competency trust over the last two decades, JIATF-S personnel have exhibited the know-how and capability to detect and monitor suspected illicit activity. A customs official shares his thoughts on how competency trust was built over time:

123 Kitfield, Anti-Drug Task Force may Provide Homeland Security Blueprint, 1/15/2010.

124 Robert M. Clark, Intelligence Analysis: A Target Centric Approach, 1st ed. (Washington D.C.: CQ Press, 2004). 8.

125 1990 Cartagena Declaration by presidents of The United States, Bolivia, Columbia, & Peru committed them to implement or strengthen a comprehensive, intensified anti-narcotics program. A tripart MOU for operations with the Bahamas, Turks, and Caicos Islands was signed in 1990 to conduct counternarcotics operations against smugglers operating within the waters of these islands. PPD 14 directed review of C2 and Intel Centers involved in international counternarcotics operations. Additionally, Liaison officers from Argentina, Brazil, Columbia, Ecuador, Peru, and Venezuela are stationed at JIATF-SOUTH to facilitate collaboration and coordinate efforts.

> When I first arrived at JIATF-S years ago, it was a lot harder to get agencies such as the DEA, Customs, and the FBI to share intelligence, for fear that sources and methods might be compromised. Increasingly, however, law enforcement agencies began to realize just what an incredible tool was being offered in terms of the intelligence capability of the Pentagon and national intelligence agencies. That realization made us want to take part in JIATF-S. This is the only place today you can get a common tactical picture based on intelligence fused from virtually every U.S. law enforcement, intelligence, and military agency.[126]

Operating in a joint and international environment where resources are scarce and response to a potential contact can carry high costs, it can be assumed that competence trust is present within the JIATF-S organization. If it were not, the majority of threat-warning tippers would go unchecked and the response from partner nations would be less because the validity of the information would be questioned and scrutinized. Therefore, information sharing and openness within the command has presumably played an integral role in building high levels of competence trust across the organization. Information sharing barriers, which plague most agencies, have for the most part been dissolved within JIATF-S by bringing in liaison officers from every contributing agency. Liaison officers provide the face-to-face contact that is essential in planning and conducting complex operations. Particularly sensitive information is generally handled by voice communication between individuals with trusted relationships. The inter-personal trust that has been established has essentially dissolved agency barriers to information sharing. Additionally, agencies tend to assign more senior personnel who are more willing to set institutional biases aside for the sake of the mission, thus, JIATF-S has evolved from a directive organization to a cooperative organization.

In the early stages of the development of JIATF-S, it became apparent that creating too many restrictions and demands on information sharing would likely impede cooperation and coordination amongst the task force participants. Therefore, each agency that originates the intelligence is given "...considerable latitude in deciding how this

126 Kitfield, Anti-Drug Task Force may Provide Homeland Security Blueprint, 4.

intelligence will be disseminated to others at the task force."[127] Thus, the onus is on the respected agency to contribute to the collective whole and fuse intelligence into a common tactical picture.

3. Leadership Design Within JIATF-S

The unique command design within the JIATF-S organization is another key attribute that lends to supporting a trusted environment. In the early stages of development, leadership began with a U.S. Navy command slant and matured into a U.S. Coast Guard Flag Officer appointed as Director assisted by a Vice Director from law enforcement. To achieve synergy and a trusted environment, the title "Commander" of the task force was changed to "Director" to merge cultures from a DoD-centric model that was stifling synergy and harboring individual agency turf concerns. The Director of JIATF-S still reports directly to the Commander of USSOUTHCOM, but as the designated leader of a reporting joint headquarters, not as a subordinate field commander. The Director, in reality, has numerous bosses outside DoD depending on the criteria of any given mission.

Leadership roles throughout all departments within JIATF-S are filled by participating agencies (see Figure 4). A complete, integrated and shared approach is the ideal model for a collaborative command structure design to facilitate a trust bond between task force participants. "This integration promotes trust and facilitates the sharing of law enforcement investigative information, which is critical for any intelligence-driven organization."[128] Key leadership positions are shared amongst the participants. "Both the Directors of Intelligence and Operations are military officers, but their Deputies are from the Drug Enforcement Agency and Customs and Border Protection."[129] Consideration for each organization is taken into account when assigning positions throughout the command. For instance, "…if DEA agents have concerns about sharing sensitive information with allied military partners, they have a certain level of

127 Kitfield, Anti-Drug Task Force may Provide Homeland Security Blueprint, 4.

128 Ibid.

129 Ibid

confidence [competence trust] that the DEA Deputy Director for Intelligence will understand those concerns."[130] Therefore, each organization feels their interests are being considered and protected, thus establishing ethical trust amongst the collective whole. This trust will remain high as long as a balance of power remains throughout the command structure and each agency feels their needs and requirements are integrated in the command design.

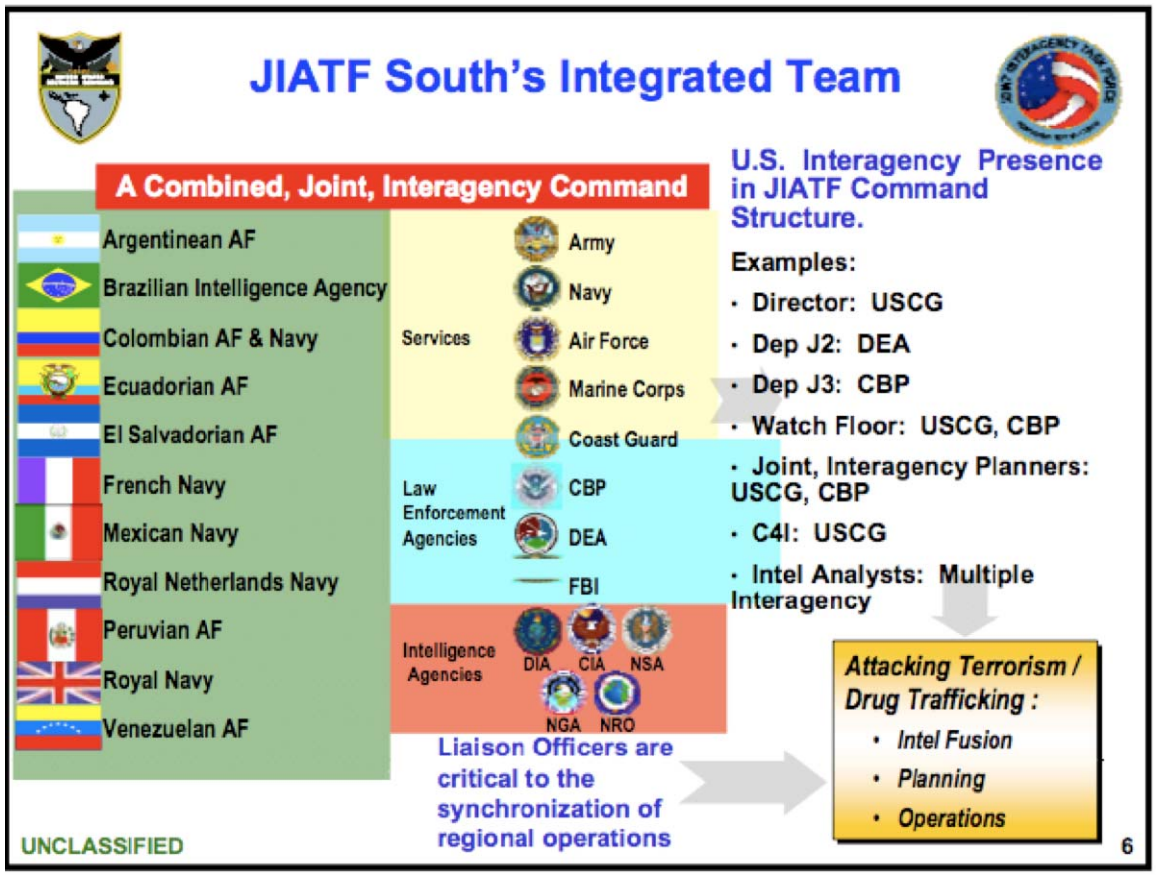

Figure 4. From Insights and Best Practices, JIATF-SOUTH Integrated Command Model[131]

130 Kitfield, Anti-Drug Task Force may Provide Homeland Security Blueprint, 4.

131 Gary Luck and Mike Findlay, Intergovernmental, and Nongovernmental Coordination, A Joint Force Operational Perspective (Norfolk, VA: Joint Warfighting Center United States Joint Forces Command, (2007).

4. Communication Methods and Feedback Within JIATF-S

JIATF-S collaborative command structure eliminates the typical agency stove-pipe mentality that is all too often prevalent within intelligence agencies. The unique design enables an integrated approach to addressing a common concern for each contributing organization. JIATF-S is a prime example of an agency that has developed and transformed after two decades of integrated operations. The JIATF-S model is not an overnight success by any means. The diversity of the participating group brings about its own challenges. Building the inter-personal relationships needed to combat narco-trafficking has been a learning experience, but vital to the successful collaborative environment that has developed. One senior government official shares his perspective on inter-personal relationships with an inter-agency environment: "The greatest system in the world does not overcome jerks and jerks will kill the greatest system in the world. And if people know each other and work together well, you don't need the system."[132] Each agency participating within JIATF-S is aware they cannot achieve success in this theater without the contribution of each and every organization participating, or at least without degrading overall capabilities.

The cornerstone of JIATF-S is the central command center that hosts representatives and liaison officers from all participating agencies and nations. The ability to be co-located not only breaks down the physical walls that separate each agency, it enables an ideal environment that supports inter-personal relationship development to build all three types of the common trust threads—competence, and ethical and emotional trust. Blending so many different agencies is not an easy task, but with time, JIATF-S has managed to work through these hurdles, by defining mission objectives, developing inter-personal trust through the partnerships with liaison officers, and open communication and information sharing that supports a unified response to narco-trafficking. These combined operations would not be possible without a merger of operations (e.g., law enforcement) and intelligence support. A task force official states,

132 Marcy Stahl, Joint Interagency Coordination Group (JIACG) Training and Education Survey Results (Vienna, Virginia: Thought Link, (2004), http://www.thoughtlink.com/files/html-docs/TLI-IITSEC02-IATrEdu_slides_files/v3_document.htm (accessed 1/28/2010).

"Today, most (about 90%) of DoD's actionable intelligence comes from law enforcement sources."[133] The evolution of DoD's role within JIATF-S has been a key component to the success within JIATF-S. This evolution process has resulted in the DoD acting in more of a supporting role versus a supported role within JIATF-S. This required a tremendous cultural shift for the DoD to relinquish the reigns of its traditional role of lead agency for the sake of the unified mission. Once this relationship was tested and found to be successful, the DoD has moderated its role within JIATF-S and actively fills a supporting role, as required.

A trust bond must exist for such a complex process of correlating and disseminating intelligence to take place. This is possible because a "Clear set of objectives [have been] agreed upon at the Principals' level."[134] And while metrics for successful operations will vary between each organization, JIATF-S has developed an understanding of the capabilities and limitations of each organization to avoid miscalculations in their planning and responses to operations. Recognizing that each contributing command has unique requirements and different definitions of success in counter-narcotics, the unified goal of stopping narco-trafficking is what aligns each and every organization that participates in the task force.

The Air Bridge Denial (ABD) program between the United States and Colombia provides an excellent example of communication failure and the necessity of defining parameters and guidelines to operate by. The ABD program was established to interdict drug traffickers moving illegal drugs by aircraft in and out of Colombia to other South American countries. This is referred to as the "air bridge."[135] To reduce this drug trafficking, the United States began operating ABD in the 1990s in Colombia and Peru.[136] The ABD program was designed to be a coordinated process where intelligence

133 Steven Shepard, "Developing Military Interagency Experts: The Next Hurdle" Air Force Command Staff College).

134 Ibid.

135 United States Government Accountability Office, Air Bridge Denial Program in Colombia has Implemented New Safeguards, but its Effect on Drug Trafficking is Not Clear (Washington D.C.: United State Government Accountability Office (2005), http://www.gao.gov/new.items/d05970.pdf (accessed 1/27/2010).

136 United States Government Accountability Office, *Air Bridge Denial Program.*

derived from JIATF-S over the horizon radar and other sources would support Colombian officials in identifying suspected aircraft potentially involved in drug trafficking. The program, however, faced setbacks in 2001 after the shooting down of a civilian aircraft in Peru.[137] The United States Government Accountability Office conducted an official review and found communication, or the lack thereof, played a large role in the accidental shoot down of the civilian aircraft. Following this horrific event, new guidelines were put in place to address the communication faults that contributed to this egregious error. A letter of agreement was signed between Columbia and the United States, which outlined each nation's responsibility to provide safe operating conditions.[138] Designated safety personnel (a total of three), including a representative from JIATF-S, oversee each mission and each have the authority to stop a mission if safety is a concern.[139] To ensure that these safeguard mechanisms are implemented, a designated communication line is required before every mission.[140] In addition to providing safeguards, each safety monitor, crewmember, weapons controller, and ground support element must be fluent in both Spanish and English. The GAO found that, "The aircrews involved in the Peru accident had flown on previous operational mission together... however, they were not proficient enough to communicate clearly during the high stress of an interception."[141] Understanding the limitations of your partner nations and agencies and identifying methods to communicate are essential for establishing all three trust threads; the failure to do so in any operation could damage your credibility (competence) your intent (ethical) and having to deal with the outcome (emotional).

B. FAILURE TO CREATE COLLABORATIVE ENVIRONMENT—NOVEMBER 2008 MUMBAI ATTACKS

The 26–29 November 2008 terrorist attack on Mumbai resulted in 165 deaths, including six Americans, and injured over 300 innocent civilians. Terrorists effectively

137 United States Government Accountability Office, *Air Bridge Denial Program.*

138 Ibid.

139 Ibid.

140 Ibid.

141 Ibid.

used highly mobile tactical assault teams to conduct simultaneous attacks on multiple targets in a crowded population center, thus exploiting soft targets, overwhelming first responders, and increasing the death counts. Reports following the event indicate the Pakistani Lashkar-e-Tayyiba operatives charged with committing the siege used a maritime insertion into Mumbai to avoid Indian authorities and capitalize on the element of surprise. The maritime insertion enabled the terrorists to reach Mumbai's population center and achieve tactical surprise with relative ease. Armed with assault rifles, handguns, grenades and IEDs, ten terrorists operating in autonomous teams were able to shut down a city of 20 million for almost four days.

India's divided network of government agencies, intelligence services, and poorly trained local police served as the weak links in this catastrophic event. The lack of a trusted collaborative network voided any threat warning that was available from reaching first responders and potential targets.[142] Chief of India's Naval Staff, Admiral Sureesh Mehta, claims, "The attacks exposed holes in intelligence-gathering and joint security action."[143] This first-hand account offers a view of the rigid dichotomy between Indian national intelligence services and local/regional law enforcement communication. Shortly after the attack, the Commander-in-Chief of Western Naval Command noted that all available assets were ordered to locate the mother ship, which aided in delivery of the LET terrorists. He stated, "If even a percentage of these very forces were deployed in a coordinated manner earlier based on the intelligence that was available, there was a good chance of thwarting the attack."[144]

The Mumbai attack is the not the worst attack in Indian history, however, its success in terrorizing an entire city for multiple days is why it is often referred to as India's 9/11 attack. The multiple attacks and the prolonged nature of the catastrophic

142 Angel Rabasa and others, *The Lessons of Mumbai* (Los Angeles: RAND Corp. (2009), http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf (accessed 6/8/2009).

143 Defense News Staff, "Plugging Maritime Security Holes - Indian, U.S. Officials Glean Lessons from Mumbai Attacks," 2008, 1/29/2010, http://www.defensenews.com/story.php?i=3853662 (accessed 1/29/2010).

144 R. S. Vasan, "Maritime Dimensions of Mumbai Terrorist Attacks on 27th November 2008," South Asia Analysis Group, no. 2957, http://www.southasiaanalysis.org/\papers30\paper2957.html (accessed 1/29/2010).

event created a worldwide audience in complete shock as to how such a low tech, small group could cause so much harm to so many.[145] Additionally, this attack has had effects on large cities with maritime access worldwide, revealing how susceptible the maritime domain can be without a coordinated effort to guard it.

India's response, during the 60-hour siege of Mumbai, highlighted key weaknesses in information sharing, command and control, and proper training, tactics and procedures for coordinating between multiple agencies in India. While not conclusive, the following list summarizes and highlights two major failures in India's response to handling the crisis management of the Mumbai attacks:

1. Intelligence dissemination on an imminent attack against Mumbai was not shared with the proper authorities or potential targets.[146] "…criticism that fishermen, the Home Ministry and foreign and domestic intelligence agencies all recorded strange chatter or received warnings of imminent attacks that were never acted upon."[147] This intelligence was also never shared or corroborated with local law enforcement officials, nor was there a central nerve center where coordinated efforts took place amongst all maritime stakeholders.

2. For the first five hours, there was no unified command structure or coordination process in place to address an attack of this magnitude.[148] Mumbai lost three of its top anti-terrorism officials almost immediately when the violence began; they were gunned down as they rode together in a van.

While this is not an exhaustive list of Indian failures in response to the Mumbai attacks, it does offer a glimpse of the glaring inadequacies of India's ability to create a trusted collaborative environment and its failure to communicate critical maritime

145 Angel Rabasa and others, *The Lessons of Mumbai.*

146 Ibid.

147 Mark Magnier, "Systemic Failure seen in India's Response to Attacks," *Los Angeles Times*, 1/12/2008, http://www.latimes.com/news/nationworld/world/la-fg-india1-2008dec01,0,1130306.story (accessed 6/8/2009).

148 John Wilson and others, Mumbai Attacks: Lessons & Responses (New Delhi, India: Observer Research Foundation, (2009), http://www.observerindia.com/cms/export/orfonline/modules/report/attachments/Mumbai%20attack_12305 52332507.pdf (accessed 6/8/2009).

intelligence in a time-sensitive manner with local/regional law enforcement officials. It also raises the question of how the United States' national intelligence services would coordinate and disseminate maritime intelligence to the right people in a similarly styled threat environment. The National Maritime Intelligence Center is designated the clearing-house for national maritime intelligence, however, the paths for distribution and coordination are still unclear. The Mumbai attacks offer lessons learned that designing and implementing a collaborative environment post-mortem is not ideal. While India has created Multiple Agency Centers (MACS) to coordinate information sharing amongst agencies, the resentment and lack of trust that now exists between India's local, regional and national agencies is likely extremely high, and the process of establishing a strong working relationship that involves information sharing will probably take an extended period of time.[149]

149 IANS, "Multi-Agency Centre Fully Operational, Next Step to Link States: Chidambaram (Lead)," *Thaindian News*, http://www.thaindian.com/newsportal/world-news/multi-agency-centre-fully-operational-next-step-to-link-states-chidambaram-lead_100149578.html (accessed 1/29/2010).

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

In these examples of law enforcement and maritime intelligence, we see that the theoretical propositions of trust claimed by leading scholars are relevant and necessary in an interagency environment. Interagency organizations must engender trust by encouraging trust-facilitating behavior at an inter-personal level as well as at an organizational level. While each member of an inter-agency force must commit to principles such as Covey's four principles of trust, the organization as a whole must organize to facilitate accountability, reciprocal trust, and transparency in order to communicate effectively. Providing empirical evidence of inter-personal trust is quite difficult and the examples provided here were only anecdotal, but the structures of organizational trust can be identified clearly in this interagency example. Furthermore, while the sampling of the case studies presented was not exhaustive, the evidence of the structural factors of organizational trust in them are provocative and demonstrate that a growing number of agencies understand and are working towards a more comprehensive implementation of theoretical components of trust in their interagency relationships.

It would be difficult to argue with the success JIATF-S has achieved in creating a trusted environment to date. It has indeed been successful at unifying diametrically opposed agency cultures and achieving a trusted environment in order to address a national objective. Leveraging shared interests to foster relationships and build trust has been the cornerstone of this organization and offers many lessons for establishing a trusted environment. The value of analyzing JIATF-S comes from examining the barriers that were broken down over time in regards to information sharing and the development of trust that flourishes within the organization today. While there has never been a shortage of national attention and emphasis on the mission of counter-narcotics, this does not explain why the same emphasis has never been applied to creating an inter-agency coordination process or national guidance that supports similar objectives. Without a thorough review of JIATF-S lessons learned, other national mission objectives, like maritime domain awareness, will most likely have to go through the same growing pains and multiple re-organization processes in the hope of someday achieving mission

success. A value set must be placed on educating intelligence professionals on the value of inter-agency operations and the necessity of an inter-agency trusted approach in today's threat environment. With today's complex mission sets, conflicts do not end by defeating an enemy force or by simply capturing rogue pirates. The threats U.S. forces face today peel back like an onion, revealing multiple layers of conflict and additional mission sets, which inherently add additional intelligence requirements that often reach beyond the scope and training of the U.S. military intelligence services. It is imperative that intelligence services learn to operate within an interagency environment so that information sharing, or the lack thereof, does not delay a response to a crisis situation. A failure to do so could potentially weaken the intelligence community's utility to decision makers and may result in missed opportunities to thwart an attack on U.S. soil.

The National Maritime Intelligence Center has taken on a tremendous amount of responsibility to serve as the national hub for maritime intelligence. One variable that will be critical to the success of the NMIC is whether they are able to identify and communicate with the maritime community as a whole. An aggressive outreach initiative program is essential for identifying the needs and requirements that exist within the maritime community, with regards to homeland security, in order to understand the releasability issues and the procedures needed to communicate and build a trusted working relationship. With that said, the NMIC must think in terms of inclusion, rather than exclusion, with its stakeholders during its intelligence production phases. As the JIATF-S case study showed, this mindset is imperative to building ethical trust within an inter-agency environment.

The JIATF-S case study also revealed the success of having a centralized command center that was staffed and led by members of participating agencies. While this is certainly an endeavor the NMIC should attempt to implement, there will be members of the maritime community that will be financially constrained to do so. That being said, the NMIC should focus on creating other avenues of information sharing with the maritime community in order to create an environment of trust. Should the NMIC provide liaison officers to all state fusion centers that have a maritime responsibility?

Questions like this will have to be hashed out, but are important because the focus should not be on creating the standard uniformed agency, but on creating an agency accessible to those in need of maritime intelligence.

The mindset of write-for-release is a concept that has been recommended numerous times following the attacks on September 11, 2001. Writing for release to your interagency partners creates avenues for collaboration and allows partners to interact, inform, and share information in a timely fashion. This in turn ensures all partners maintain shared situational awareness and have access to all relevant threat information. While this is only one avenue to explore for information sharing, it offers key insights into the thought process of identifying with the stakeholders to establish trust and understand their needs and capabilities. Keeping with the traditional ad-hoc, and largely personality driven (good ol' boy), way of information sharing amongst agencies that has existed for sometime, is not ideal and will most likely result in failure to create trust in any environment. Today's inter-agency environment requires engagement at all levels, both multilevel and multifarious. Establishing a trusted inter-agency collaborative environment in today's threat environment will ultimately be the deciding factor of intelligence relevance or failure.

A. FURTHER RESEARCH

This thesis was heavily focused on creating trust within an organization. Other collaborative models exist that have helped organizations achieve a collaborative environment with their external partners and these are worth exploring in an effort to understand the utility of creating an alternative to the environment prescribed in this thesis. One model, in particular, is the New York Police Department (NYPD) SHIELD program that connects intelligence and critical infrastructure professionals with private business security firms and concerned citizens. This design is interesting because while there is no centralized command center for security representatives throughout New York City, NYPD SHIELD connects with its private security partners through outreach officers. These officers offer on-site inspections and assistance with regard to security and vulnerability assessments, and through an interactive web portal that is constantly

updated with threat information, vulnerability assessments and intelligence analysis of world events and the implications for New York City. What is unknown about this case study is whether security professionals are operating out of necessity, following the horrific events of 9/11 (without a trusted environment), or as a collaborative whole (trusted environment) that realizes a trusted environment is necessary to piece scarce threat information together. This is worth exploring if it does, in fact, create a trusted environment, as a potential alternative design for organizations such as the NMIC to study and utilize in an inter-agency environment.

Regardless of the design model, organizational and interpersonal trust has been identified as a pivotal factor for establishing collaboration in both the private and public sectors. Breaking down cultural divides requires an all-hands approach. The results of a trusted interagency operational culture will support its effectiveness in the same fashion joint operations have in traditional military operations. The National Maritime Intelligence center has continued to transform and evolve to meet the challenges of the 21st century. The organizational and cultural products of true inter-agency trusted collaboration possess many salient characteristics that the interagency community and its partners will need to address the challenges of today's national security concerns. "Inter-agency operations hold the same promise that amphibious operations did a century ago: Victory."[150]

150 Matthew Bogdanos, Transforming Joint Interagency Coordination: The Missing Link between National Strategy & Operational Success (Washington D.C.: Center for Technology and National Security Policy (2007).

BIBLIOGRAPHY

Berry, A. G. "The Beginning of the Office of Naval Intelligence." *U.S. Naval Institute Proceedings,* no. 63 (1/1937): 102.

Bogdanos, Matthew. *Transforming Joint Interagency Coordination: The Missing Link between National Strategy & Operational Success*. Washington DC: Center for Technology and National Security Policy, 2007.

Brooks, Rosa. "War on Terror an Exercise in Folly," *Los Angeles Times*, 12/4/2008, sec. Opinion.

Clark, Robert M. *Intelligence Analysis: A Target Centric Approach*. 1st ed. Washington DC: CQ Press, 2004.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. http://govinfo.library.unt.edu/wmd/report/index.html (accessed 5/15/2009).

Carafano, James Jay. "Interagency Dialogue: Managing Mayhem: The future of Interagency Reform," *Joint Forces Quarterly*, no. 49, 2nd Quarter, 2008, 135–137.

Covey, Stephen. *The Speed of Trust, the One Thing that Changes Everything*. New York, NY: Free Press, 2006.

Defense News Staff. Plugging Maritime Security Holes — Indian, U.S. Officials Glean Lessons from Mumbai Attacks, 2008, 1/29/2010.

Dickey, Christopher. *Securing the City, Inside America's Best Counterterror Force-the NYPD*. New York, NY: Simon & Schuster, 2009.

Director, National Counter Terrorism Center. *NCTC and Information Sharing: Five Years since 9/11, A Progress Report*. Washington DC: National Counter Terrorism Center, 2006.

Dorwart, Jeffery. *The Office of Naval Intelligence, the Birth of America's First Intelligence Agency 1865–1918,* Naval Institute Press, 1979.

Dragonette, Charles. "Rescuing the M/V Maersk Alabama, ONI Leadership in Counter-Piracy Analysis." *The ONI Quarterly* (5/2009).

Garner, Dwight. "Books of the Times - Police Beat the Terrorists with Big Stick and Brains in Christopher Dickey's 'Securing the City' - Review - NYTimes.Com." NYTimes.com. http://www.nytimes.com/2009/02/04/books/04garn.html (accessed 5/20/2009).

Hall, Tamara. *Intelligence Community Collaboration Baseline Stud*y. MITRE Corporation, 1999.

Hamilton, Lee. “Hamilton Shares Thoughts on 9/11.” http://www.homepages.indiana.edu/102204/text/hamilton.shtml (accessed 5/15/2009).

House Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection. *Testimony of New York City Police Commissioner Raymond W. Kelly: The Mumbai Attacks: A Wake-Up Call for America's Private Sector*, 3/11/2009.

IANS. “Multi-Agency Centre Fully Operational, Next Step to Link States: Chidambaram (Lead).” *Thaindian News*. http://www.thaindian.com/newsportal/world-news/multi-agency-centre-fully-operational-next-step-to-link-states-chidambaram-lead_100149578.html (accessed 1/29/2010).

———. “US Warned India Twice of Mumbai Attack by Sea a Month Ago.” *Thaindian News.* http://www.thaindian.com/newsportal/world-news/us-warned-india-twice-of-mumbai-attack-by-sea-a-month-ago-reports-lead_100126422.html (accessed 5/18/2009).

Joint Publication 3-08. “Interagency, Intergovernmental, Nongovernmental Organization Coordination During Joint Operations Vol. I.” 3/17/2006. www.js.pentagon.mil/doctrine/jel/new_pubs/jp3_08v1.pdf (accessed: 09/28/2009).

King, David, and Zachary Krabell. *The Generation of Trust: Public Confidence in the U.S. Military Since Vietnam.* Washington DC: The AEI Press, 2003.

Kitfield, James. “Anti-Drug Task Force may Provide Homeland Security Blueprint.” *National Journa*l (9/20/2002), http://www.govexec.com/dailyfed/0902/092002nj1.htm (accessed 1/15/2010).

Kreisher, Otto. “Collaborative Approach, U.S. Maritime Operational Threat Response Plan Coordinates Federal Action in Ports and Far from Shore.” *Seapower* (5/2009).

Luck, Gary, and Mike Findla*y.* “Intergovernmental, and Nongovernmental Coordination, A Joint Force Operational Perspective.” Focus Paper (Norfolk, VA: Joint Warfighting Center United States Joint Forces Command, 2007.)

Magnier, Mark. “Systemic Failure seen in India's Response to Attacks,” *Los Angeles Times*, 12/1/2008.

McNamara, Regina, CDR USCG. *Ribbon Cutting Establishes the New National Maritime Intelligence Center*. Washington D.C.: Pentagon Press Release, http://www.navintpro.org/associations/4202/files/quarterly/NIPQIndex.htm (accessed 6/9/2009).

McNamara, Thomas. *Information Sharing Environment, Progress and Plans, Annual Report to the Congress*, 2009.

National Commission on Terrorist Attacks. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton, 2004.

Office of The Director of National Intelligence. *Intelligence Community Directive 205: Analytic Outreach*. Washington DC: 2008a.

_____. *United States Intelligence Community: Information Sharing Strategy*. Washington D.C.: 2008b.

Office of Naval Information. "Transforming Naval Intelligence." *Rhumb Lines, Strait Lines to Navigate by* (2/24/2009, http://www.navy.mil/navco/speakers/currents/Transforming_Naval_Intelligence_27_FEB_09_FINAL.pdf (accessed 1/6/2010).

Packard, Wyman. *A Century of U.S. Naval Intelligence*. Washington DC: Department of the Navy, 1996.

Prange, Gordon. *At Dawn We Slept: The Untold Story of Pearl Harbor*. 1st ed. McGraw-Hill, 1981.

Rabasa, Angel, Robert Blackwill, Peter Chalk, Kim Cragin, Christine Fair, Brian Jackson, Brian Jenkins, Seth Jones, Nathaniel Shestak, and Ashley Tellis. *The Lessons of Mumbai*. Los Angeles: RAND Corp., 2009.

Romahn, Elke and Francis Hartman. "Trust: A New Tool for Project Mangers," Philadelphia, Pennsylvania, 10/10-16/1999.

Rosen, Evan. *The Culture of Collaboration*. 1st ed. San Francisco, CA: Red Ape Publishing, 2007.

Russell, Anthony. "Statement by Adm. Thad Allen, Commandant of the Coast Guard, on Piracy." United States Coast Guard. http://www.piersystem.com/go/doc/786/268323/ (accessed 1/6/2010).

Schobel, Markus. "Trust in High-Reliability Organizations." *Social Science Information* 48 (2009): 315.

Shepard, Steven. “Developing Military Interagency Experts: The Next Hurdle.” Air Force Command Staff College, 2006.

Stahl, Marc*y. Joint Interagency Coordination Group (JIACG) Training and Education Survey Results*. Vienna, Virginia: Thought Link, 2004.

Stevenson, William. “Organization Design.” In *Handbook of Organizational Behavior*, 2nd ed. Ed Robert T. Golembiewski. New York, NY: Marcel Dekker, Inc., 2001. 145–174.

Sully, James, SGT. *Personal e-mail concerning Command Workshop for Common Ground Exercise in LA Count*y. Los Angeles Sheriffs Dept Hosting a Mumbai Style Attack Exercise in LA County to Test Unified Command Structure.

Sztompka, Piotr. *Trust: A Sociological Theory*. Cambridge: Cambridge University Press, 1999.

Treverton, Gregory. “Intelligence Test: Post 9/11 Intel Reform Has Been in Name Only. To Make America Safer, We Need Fundamental Change Across the Entire Government.” *Democracy: A Journal of Idea*s Winter 2009, no. 11, http://www.democracyjournal.org/article.php?ID=6667 (accessed 5/15/2009).

——— and Peter Wilson. “True Intelligence Reform is Cultural, Not just Organizational Chart Shift.” *The Christian Science Monito*r (1/13/2005, www.rand.org/commentary/2005/01/13/CSM.html (accessed 5/15/2009).

Tucker, D. (Autumn 2000). The RMA and the interagency: Knowledge and Speed vs. Ignorance and Sloth? *Parameters, XXX* (3), 66–76.

United Kingdom House of Commons. *The Butler Report - Review of Intelligence on Weapons of Mass Destruction*. London, England: House of Commons, 2004.

The United States Congress. *Senate Intelligence Committee on Intelligence –- Postwar Finding's on Iraq's WMD Programs and Links to Terrorism and How They Compare with Prewar Assessments*. Washington D.C.: United States Congress, 2006.

The United States Department of Homeland Security. *Department of Homeland Security Information Sharing Strateg*y. Washington D.C.: Department of Homeland Security, 2008.

———. *National Concept of Operations for Maritime Domain Awarenes*s, 2007.

———. *The National Strategy for Maritime Securit*y, 2005.

———. *Maritime Operational Threat Response Plan for the National Strategy for Maritime Securit*y, 2006.

The United States Government. *National Strategy for Information Sharin*g. Washington D.C.: White House, 2007.

The United States Government Accountability Offic*e. Air Bridge Denial Program in Colombia Has Implemented New Safeguards, But Its Effect on Drug Trafficking is Not Clear*. Washington D.C.: United State Government Accountability Office, 2005.

The United States Senate Committee on Governmental Affairs. *Summary of Intelligence Reform and Terrorism Prevention Act of 200*4. Washington D.C.: Congress, 2004.

The United States Senate Committee on Homeland Security & Governmental Affairs. *Testimony of New York City Police Commissioner Raymond W. Kelly: Lessons from the Mumbai Terrorist Attacks.* 1/8/2008.

Van de Ven, Andrew, and Peter Smith Ring. "Relying on trust in cooperative inter-organizational relationships." In *Handbook of Trust Research*. Ed. Reinhard Bachmann & Akbar Zaheer. Northampton, MA: Edward Elgar, 2006, 144–164.

Vasan, R. S. "Maritime Dimensions of Mumbai Terrorist Attacks on 27th November 2008." *South Asia Analysis Group*, no. 2957, http://www.southasiaanalysis.org/\papers30\paper2957.html (accessed 1/29/2010).

Wilson, John, Paul Soren, Anjali Sharma, Joyeeta Bhattacharjee, Kaustavdhar Chakrabarti, Aashti Salman, and Nisha Verma. *Mumbai Attacks: Lessons & Response*s. New Delhi, India: Observer Research Foundation, 2009.

Yeatman, Richard. "JIATF-South, Blueprint for Success." *Joint Forces Quarterly,* no. 42 (2006).

Zeichner, Lee M. "Legal Foundations: Public Trust and Confidence in Critical Infrastructure." *The CIP Report 4, no. 11,* 5/2006, 3–4, 13.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, New Jersey: Princeton University Press, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California